Auftragsverarbeitungsvertrag nach DSGVO

Stand: 06/2019

zwischen

vertreten durch

im Folgenden Auftraggeber genannt

und

Förderverein des Freilichtmuseums am Kiekeberg e.V.
Am Kiekeberg 1
21224 Rosengarten-Ehestorf

Vorsitzender: Heiner Schönecke (MdL)

Vereinsregister: Amtsgericht Lüneburg

Register-Nr. 110393

im Folgenden Auftragnehmer genannt

1. Gegenstand des Auftrages
Der Gegenstand des Auftrages ergibt sich durch die Leistungsbeschreibung in Anlage 2.

2. Allgemeines

2.1. Dieser Auftragsverarbeitungs-Vertrag (**AVV**) regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers lt. Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (**DSGVO**).

2.2. Sofern in dieser AVV der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ lt. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2.3. Es ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogenen Daten bekommt bzw. Kenntnis erlangt, da der Auftragnehmer im Auftrag des Auftraggebers vor Ort oder per Fernwartung Wartungs- und/oder Pflegearbeiten, Installationsarbeiten und Konfigurationsarbeiten und/oder Überwachungen der IT-Systeme an IT-Systemen des Auftraggebers durchführt.

2.4. Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Informationstechnologie; IT- Service sowie Dienstleitungen, die entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z.B. BGB) basieren. Gegebenenfalls erbringt der Auftragnehmer weitere Leistungen in der Zukunft, die in der Zukunft gesondert beauftragt werden.

3. Fernwartung

3.1. Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen und ggf. abzubrechen.

3.2. Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht lt. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung lt. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

3.3. Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

4. Art der Daten
Hierbei ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Daten/Datenarten hat:

4.1. Personenstammdaten (Personal, Kunden, Lieferanten und sonstige Partner)
4.1.1. Kommunikationsdaten (z.B. Telefon, E-Mail)
4.1.2. Vertragsstammdaten
4.1.3. Bankdaten
4.1.4. Vertragsabrechnungs- und Zahlungsdaten
4.2. Nutzdaten
4.3. Kundenhistorie
4.4. Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

5. Kreis der Betroffenen
5.1. Kunden
5.2. Lieferanten
5.3. Interessenten
5.4. Mitarbeiter
5.5. Handelsvertreter
5.6. Abonnenten
5.7. Sonstige Adressaten

6. Rechte und Pflichten des Auftraggebers

6.1. Der Auftraggeber ist, so lange er allein über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, alleiniger Verantwortlicher lt. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten die im Auftrag durch den Auftragnehmer durchgeführt werden.

6.2. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen. Mündlich erteilte Weisungen werden in Schriftform bestätigt.

6.3. Dem Auftragnehmer steht das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist und die Verarbeitung solange auszusetzen, bis der Auftraggeber die Weisungen anpasst oder bestätigt.

6.4. Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich. Der Auftragnehmer wird den Auftraggeber hierbei unterstützen.

6.5. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

6.6. Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht lt. § 203 StGB unterliegt, gilt der Auftragnehmer als Gehilfe lt. § 203 StGB und unterliegt der gleichen Berufsgeheimnisverpflichtung. Der Auftraggeber hat den Auftragnehmer diesbezüglich zu informieren.

6.7. Der Auftraggeber kann weisungsberechtigte Personen benennen. Für den Fall, dass sich die schriftlich benannten weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer umgehend in Textform mitteilen.

6.8. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

7. Allgemeine Pflichten des Auftragnehmers

7.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen, soweit gesetzlich zulässig.

7.2. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach dem Dienstleistungsvertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat oder eine gesetzliche Verpflichtung besteht.

7.3. Der Auftragnehmer wird den Auftraggeber, der für die Wahrung der Betroffenenrechte verantwortlich ist, unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

7.4. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung bis zu einer Klärung der Haftung auszusetzen.

7.5. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Ausnahmen sind vom Auftraggeber schriftlich zu genehmigen.

7.6. Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform zulässig.

7.7. Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

7.8. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

7.9. Der Auftragnehmer sichert die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

7.10. Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete besondere Arten bzw. besondere Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO oder personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

7.11. Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

8. Datenschutzbeauftragter des Auftragnehmers

8.1. Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat, wenn dies gesetzlich vorgeschrieben ist. Sobald ein Datenschutzbeauftragter bestellt ist, trägt der Auftragnehmer dafür Sorge, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Sofern ein betrieblicher Datenschutzbeauftragter bestellt wurde, wird der Auftragnehmer diesen in Anlage 3 entsprechend benennen.

9. Meldepflichten des Auftragnehmers

9.1. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

9.2. Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag

des Auftraggebers erbringt, betreffen kann.

9.3. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird dem Auftraggeber Empfehlungen aussprechen, die dem unbefugten Zugriff auf personenbezogene Daten vorbeugen und möglichst schützen. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 72 Stunden ab Kenntnis des Zugriffs mitteilen.
Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

10. Mitwirkungspflichten des Auftragnehmers

10.1. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO.

10.2. Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

10.3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

10.4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen oder Unterstützung im Zusammenhang der Punkte 10.1 – 10.3 dieses Vertrages beim Auftragnehmer entstehen, bleiben unberührt.

11. Kontrollbefugnisse

11.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

11.2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle lt. Punkt 11.1 dieses Vertrages erforderlich ist.

11.3. Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

11.4. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Punktes 11.1 dieses Vertrages in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. 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.

11.5. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber lt. Art. 58 DSGVO i.V.m. §40 BDSG (neu), im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen.

12. Untervertragsverhältnisse

12.1. Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

12.2. Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

12.3. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Subunternehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

12.4. Die Verpflichtung des Subunternehmens muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

12.5. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer

gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

12.6. Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

12.7. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

12.8. Der Auftragnehmer ist verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

12.9. Nicht als Unterauftragsverhältnisse lt. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten

12.10. Es gelten die Regelungen in diesem Vertrag auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Die Beauftragung von Subunternehmen in Drittstaaten durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

13. Vertraulichkeitsverpflichtung

13.1. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

13.2. Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der

Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

13.3. Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

14. Wahrung von Betroffenenrechten

14.1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

14.2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – unter anderem auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

14.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

15. Geheimhaltungspflichten

15.1. Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

15.2. 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.

16. Technische und Organisatorische Maßnahmen zur Datensicherheit

16.1. Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

16.2. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 1 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit

der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

16.3. Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

17. Dauer des Auftrages

17.1. Die Dauer des Auftrags

☐ entspricht der Laufzeit des bestehenden Wartungsvertrages

☐ ist befristet bis zum _____

☐ Der Auftrag wird zur einmaligen Erbringung der in Anlage 2 beschriebenen Leistungen erteilt. Die Leistung gilt durch Abnahme durch den Auftraggeber als erbracht.

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monaten zum Quartalsende gekündigt werden.

17.2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

18. Beendigung

18.1. Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

18.2. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des

Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

19. Zurückbehaltungsrecht

19.1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer lt. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

20. Haftung

20.1. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

21. Schlussbestimmungen

21.1. Sollte das Eigentum des Auftraggebers beim 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 informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

21.2. Für Nebenabreden ist die Schriftform erforderlich.

21.3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

.....	.....
Ort/ Datum	*Ort/ Datum*
.....	.....
Unterschrift (Auftragnehmer)	*Unterschrift (Auftraggeber)*

Anlage 1 (TOM) Technische und Organisatorische Maßnahmen im Freilichtmuseum am Kiekeberg

1. Zutrittskontrolle

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle:

- Schlüssel Schließsystem
- Manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Besucher in Begleitung durch Mitarbeiter

2. Zugangskontrolle

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologien bei Remote-Zugriffen
- Schlüsselregelung (Schlüsselausgabe etc.)
- Einsatz von Anti-Viren-Software auf Servern und Clients
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall auf Servern und Clients
- Automatische Desktopsperre
- Verschlüsselung ext. Datenträger

3. Zugriffskontrolle

- Erstelltes Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortkomplexität
- Weitgehende Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern nach DIN

4. Weitergabekontrolle

- Einrichtungen VPN-Tunneln
- Beim physischen Transport: Löschen von Datenträgern vor dem Versand
- Bereitstellen über verschlüsselte Verbindungen wie sftp, https

5. Eingabekontrolle

- Bedingte Protokollierung der Eingabe, Änderung und Löschung von Daten
- Bedingte Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Verfügbarkeitskontrolle und Belastbarkeit
   - Unterbrechungsfreie Stromversorgung (USV)
   - Schutzsteckdosenleisten in Serverräumen
   - Rauchmeldeanlagen
   - Feuerlöscher in Serverräumen
   - Erstellen eines Backup- & Recovery-Konzepts
   - Kontrolle des Sicherungsvorganges
   - Testen von Datenwiederherstellung
   - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
   - Serverräume nicht unter sanitären Anlagen

7. Trennungskontrolle
   - Trennung von Produktiv- und Testumgebung
   - Mandantenfähigkeit relevanter Anwendungen
   - Festlegung von Datenbankrechten
   - Steuerung über Berechtigungskonzept

8. Pseudonymisierung
   - Die Verarbeitung personenbezogener Daten soweit möglich in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

9. Auftragskontrolle
   - Es werden keine Daten zur Verarbeitung an Dritte weitergegeben, es sei denn, sie sind zur Durchführung des Auftrages des Auftraggebers notwendig (Lizenzbestellungen, Leasing, gesetzliche Anforderungen, Lieferungen, Abrechnungen u.s.w.)
   - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz bzw. EU Standard Vertragsklauseln
   - Verpflichtung der Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei vorliegender Bestellpflicht
   - Regelung zum Einsatz weiterer Subunternehmer

Anlage 2 Leistungsbeschreibung

Die Tätigkeiten des Auftragnehmers für den Auftraggeber im Rahmen der Auftragsdatenvereinbarung sind wie folgt festgelegt:

Tätigkeiten sind dem nachfolgend benannten Vertrag zu entnehmen:

☐ FirstRumos Wartungsvertrag vom _____

☐ Anderer Vertrag: _____ vom _____

Die Tätigkeit des Auftragnehmers umfasst folgende Dienstleistungen:

☐ Pflege und Wartung der Museumssoftware FirstRumos

☐ Pflege und Wartung anderer Software des Fördervereins des Freilichtmuseums am Kiekeberg e.V.

☐ Installation und Konfiguration der für FirstRumos verwendeten IT-Systeme

☐ Hotline- und Online-Support

☐ Konvertierung und Bearbeitung von Daten sowie Import der Daten in FirstRumos

☐ Durchführung von Schulungen (mit Daten des Auftraggebers)

☐ Bereitstellung von Daten im Internet (FirstRumos Archivportal, Weitergabe an museum digital)

Weitere Beschreibungen der Leistungen:

Anlage 3: Betriebliche Datenschutzbeauftragte

Datenschutzbeauftragter des Auftraggebers:

Name:

Anschrift:

E-Mail:

Telefonnummer:

Datenschutzbeauftragter des Auftragnehmers:

Name: Andreas Woost

E-Mail: datenschutz@kiekeberg-museum.de