Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

Nutzer des webbasierten Systems „CIRIS“

- Auftraggeber -

und

Jetsam Service Management GmbH

Dr.-Leo-Ritter-Straße 4

93049 Regensburg

Deutschland

- Auftragnehmer -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 dieser Vereinbarung das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) 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.

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

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

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

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33 und 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag 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.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform (z.B. E-Mail) erfolgen muss. Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 – 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für die personenbezogenen Daten zu gewährleisten.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) 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.

(5) 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 insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder dessen Unterauftragnehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(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.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt ist/sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

6. Meldepflichten des Auftragnehmers

(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.

(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.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht im Falle von Datenschutzverletzungen nach Art. 33 und 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. 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 48 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 sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12 - 23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(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.

(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.

8. „Home-Office"-Regelung

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, mit vorheriger Zustimmung des Auftraggebers die Verarbeitung von personenbezogenen Daten in Privatwohnungen („Home-Office") erlauben. Die Zustimmung des Auftraggebers bedarf der Textform (z.B. E-Mail).

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch im „Home-Office" der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten im „Home-Office" die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen, die im „Home-Office" verwendet werden, ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere im Haushalt befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag im „Home-Office" durch den Auftraggeber möglich ist. Dabei sind die Persönlichkeitsrechte der Beschäftigten sowie der weiteren im jeweiligen Haushalt lebenden Personen angemessen zu berücksichtigen.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte im „Home-Office" eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9. Kontrollbefugnisse

(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.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

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

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 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.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere 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. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten im „Home-Office“ zur Wahrung der Persönlichkeitsrechte von Beschäftigten des Auftragnehmers und etwaiger weiterer Personen im jeweiligen Haushalt primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgen. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle im „Home-Office“ von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in **Anlage 2** zu diesem Vertrag angeben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer 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.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen 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.

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

(5) 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.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) 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.

(7) Nicht als Unterauftragsverhältnisse i.S.d. 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. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden, und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

11. Vertraulichkeitsverpflichtung

(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.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit ihrer Anwendung vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht 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 sie über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 ist dem Auftraggeber auf Anfrage nachzuweisen.

12. Wahrung von Betroffenenrechten

(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 unterstützen. Der Auftragnehmer hat dabei insbesondere 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.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere Ansprüche auf Auskunft sowie Berichtigung, Sperrung oder Löschung von Daten - 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.

(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.

(4) Für den Fall, dass ein Betroffener seine Rechte nach den Art. 12 - 23 DSGVO beim Auftragnehmer geltend macht, obwohl dies offensichtlich eine Verarbeitung personenbezogener Daten betrifft, für die der Auftraggeber verantwortlich ist, ist der Auftragnehmer berechtigt, dem Betroffenen mitzuteilen, dass der Auftraggeber der Verantwortliche für die Datenverarbeitung ist. Der Auftragnehmer darf dem Betroffenen in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

13. Geheimhaltungspflichten

(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.

(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.

14. Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

15. Technische und organisatorische Maßnahmen zur Datensicherheit

(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.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** 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 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.

(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.

16. Dauer des Auftrags

(1) Der Vertrag beginnt, sobald der Auftragnehmer dem Antrag des Auftraggebers bezüglich der Nutzung des webbasierten Systems „CIRIS“ und der Bereitstellung der Zugangsdaten zu „CIRIS“ stattgegeben hat.

(2) Er endet mit Ende der Nutzung von „CIRIS“ durch Kündigung oder zum Ende der Testphase.

(3) 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.

17. Beendigung

(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 sie 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.

(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.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

18. Zurückbehaltungsrecht

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

19. Schlussbestimmungen

(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.

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Im Rahmen der Verarbeitung von Elektro- und Elektronikaltgeräten stellt der Auftragnehmer die nötige IT-Struktur zur Verfügung, um die reibungslose und nachvollziehbare Abwicklung von der Abholung bis hin zur Entsorgung zu gewährleisten.

Die Verarbeitung der Waren obliegt dem Auftraggeber bzw. dessen Unterauftragnehmer(n) und beinhaltet Logistik, Verarbeitung der Waren und Löschung oder Zerstörung von personenbezogenen Daten, die sich auf den Waren befinden.

Weitere Details zu den vereinbarten Leistungen des Auftragnehmers sind in dem geschlossenen Servicevertrag bzw. den zugrunde liegenden AGBs einzusehen.

Die Daten werden nur zum Zweck der Erfüllung des Vertrages verarbeitet inklusive der Sicherstellung der Funktion der Systeme und deren Sicherheit.

Die Verarbeitung von personenbezogenen Daten beinhaltet zum aktuellen Zeitpunkt das System CIRIS („CIRECON Reporting and Information System“), über das die Elektro- und Elektronikaltgeräte zur Entsorgung angemeldet und der Abholstatus gesteuert wird. Zusätzlich wird nach Ankunft der Waren der Verarbeitungsstatus an den Auftraggeber gemeldet. Über das Ticketsystem OTRS werden Eskalationen und andere Kommunikation mit dem Auftraggeber sowie mit dem Unterauftragnehmer, dem Entsorger der Waren, bearbeitet. Dazu wird auch E-Mail verwendet, um weitere Informationen wie Rechnungen und Verwertungsnachweise zu versenden und zu empfangen.

Die personenbezogenen Daten sind notwendig, um den sicheren Zugang zu den Systemen zu gewährleisten, die Verantwortlichen und Ansprechpartner des Auftraggebers für die verschiedenen Prozessschritte zu benennen und einen reibungslosen Kommunikationsweg von der Anmeldung über die Bereitstellung bis hin zur Abholung und Logistik zu ermöglichen. Weiterhin werden die Daten für die Vorbereitung der Rechnungsstellung seitens des Auftraggebers gegenüber dem Verarbeiter der Ware benötigt.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Nutzerdaten (Name, Vorname, E-Mail-Adresse, Telefonnummer, Adresse)
- Verlaufsdaten in CIRIS (Datum und Nutzer, der einen Status ändert, Login-Daten)
- OTRS-Daten mit Zeitstempel und Nutzer oder E-Mail-Adresse bei der Erstellung eines Tickets, Nutzer, Bearbeiter und Uhrzeit einer Ticketbearbeitung (Statusänderung, Antwort, Schließen des Tickets etc.)
- Anmeldedaten und Uhrzeit bei Anforderung eines Accounts im Vorfeld einer Vertragsanbahnung
- Typische Log-Daten (wie IP-Adresse, Zeitstempel) des Webservers und OTRS-Servers (wenn ein Nutzer einen OTRS-Account besitzt)

3. Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

- Mitarbeiter des Auftraggebers
- Dritte (Verarbeiter der Elektro- und Elektronikaltgeräte, Logistiker)
- Mitarbeiter des Auftragnehmers

4. Weisungsberechtigte Personen des Auftraggebers

Antragsteller für den Zugang zu CIRIS im Zuge des Registrierungsvorgangs

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

Christine Gering <christine.gering@jetsam-services.de>

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

Firma:	**noris network AG**
Rechtsform:	Aktiengesellschaft
Adresse:	Thomas-Mann-Straße 16-20, 90471 Nürnberg, Deutschland
Kontakt:	Account Manager: Ibrahim Calginbas
	Tel.: +49 911 9352-1620, E-Mail: ibrahim.calginbas@noris.de
	Datenschutzansprechpartner: Christian Volkmer
	Projekt 29 GmbH & Co. KG, Ostengasse 14, 93047 Regensburg, Deutschland
	Tel.: +49 941 2986930, E-Mail: anfragen@projekt29.de
Leistung:	Rechenzentrum; Bereitstellung Hardware für
	E-Mail-, Web-, OTRS- und Datenbankserver

Anlage 3 - Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

Maßnahmen Rechenzentrum (noris):

- 24/7 Videoüberwachung mit Archivierung
- Biometrische Zutrittskontrolle mit 24/7-Zutritt mittels Transponderkarte
- Überwachung durch Sicherheitsdienst
- Rack-Überwachung mit leistungsfähigen Monitoring-Systemen
- Alarmanlage und Meldesystem für/bei unberechtigtem Zutritt
- Pförtner bzw. Leitstelle zur Überwachung vor Ort
- Zertifikate u.a.: ISO/IEC 27001: 2013

Maßnahmen Firmensitz:

- Zugang mit Token
- Zugang zu besonders relevanten Räumen (Serverräume etc.) nur mit zusätzlicher Berechtigung
- Besucher nur nach Anmeldung

Zugangskontrolle

CIRIS

Die Anfrage für einen Testzugang erfolgt über die Webseite www.cirecon.de mit automatischer Erzeugung eines OTRS-Tickets, das von Verantwortlichen des Auftragnehmers, sogenannten Super Admins, für CIRIS bearbeitet wird. Die Zusendung des Auftragsverarbeitungsvertrages an den Auftraggeber und die Zusendung der initialen Zugangsdaten erfolgt per E-Mail. Die Änderung des Passwortes obliegt dem Auftraggeber.

Die Mindestanforderungen an die Passwortlänge und an notwendige Sonderzeichen sind vorgegeben. Die Neuanlage oder Änderung der Accounts erfolgt nur, wenn sie gemäß den Vorgaben ist.

Nach Beendigung des Testzeitraums und nach Vertragsabschluss mit dem Auftraggeber wird ein Live-Account aktiviert und zur erweiterten Funktionalität durch einen Super Admin freigeschaltet. Erfolgt kein Vertragsabschluss bzw. endet der Vertrag, werden die Accounts für vier Wochen gesperrt und danach gelöscht. In der Sperrzeit kann ein Export der Daten verlangt werden.

Nach Erhalt des vollen Administrationsrechts kann der Auftraggeber selbst Mitarbeiteraccounts anlegen und bestimmen, welche Rollen (Berechtigungen) und Zugriffsrechte diese für verschiedene Module im System haben.

Die Passwortvorgaben und das Deaktivieren von Accounts werden systemseitig reguliert, unterliegen aber ansonsten der Verantwortung des Auftraggebers und dessen Datenschutzrichtlinien.

Jeder Nutzer kann sein Passwort selbst ändern. Auf Anfrage kann ein neues Passwort generiert werden, das der Nutzer wieder selbständig ändern muss.

Das Löschen von Accounts erfolgt durch den Auftragnehmer auf Anforderung des Auftraggebers.

Erfolgreiche Anmeldungen werden in der Datenbank von CIRIS gleich nach Account-Anlage protokolliert. Bei OTRS erfolgt die Zugangsfreigabe und Account-Anlage durch einen Super Admin von CIRIS.

Dienstleister sind entweder zertifiziert und weisen dadurch die entsprechende Eignung nach oder werden per Audit regelmäßig auf die Einhaltung des Umgangs mit personenbezogenen Daten überprüft.

Ein direkter Zugang zu den Datenbank- und Webservern ohne Verwendung der CIRIS-GUI ist nur mittels Active Directory Account aus dem Firmennetz bzw. über VPN des Auftragnehmers möglich. Zu den Servern mit ihren Logfiles und Datenbanken haben die Systemadministratoren Zugriff und benannte Verantwortliche für CIRIS. Die allgemeinen technischen und organisatorischen Maßnahmen (im Folgenden „TOMs“) des Auftragnehmers regeln den Zugang zu den Daten und ihre Sicherheit und die Vereinbarkeit mit der DSGVO.

Zugriffskontrolle

Benutzerrollen in CIRIS und deren Ausgestaltung obliegen dem Verantwortlichen. Der Verantwortliche ist Vertragspartner des zugrundeliegenden Dienstleistungsvertrages, bekommt den Company Account für seine Firma und kann Mitarbeiter- sowie weitere Sub-Company-Accounts für Tochterfirmen anlegen. Der Verantwortliche mit einem Company Account entscheidet über den Zugriff auf die vorhandenen Informationen für die weiteren Accounts. Der Auftragnehmer unterstützt lediglich in der korrekten Ausgestaltung der Rollen und der Abbildung der Firmenstruktur.

Nach Ablauf des Dienstleistungsvertrages erlischt der Zugang zum System für den Verantwortlichen und seine Mitarbeiter. Daten werden nach dem Vertrag und nach Ende der jeweils notwendigen Aufbewahrungsfristen entsprechend gelöscht.

Administratoren (dies beschränkt sich auf Mitarbeiter des Auftragnehmers) der Web-Applikation CIRIS können Accounts anlegen und Rollen vergeben. Auch sind sie für die Accounts im Ticketsystem verantwortlich.

Die Erstellung und Nutzung eines Administrator-Accounts in CIRIS und der Zugriff auf Daten außerhalb der Web-Applikation, wie der Zugang zu OTRS-Tickets oder zu Server-Logfiles, werden über die allgemeinen TOMs geregelt, denen alle IT-Systeme des Auftragnehmers unterliegen.

Trennung

An den Login-Daten hängen bestimmte Rollen. Nur Admins des Auftragnehmers können alle Accounts und Inhalte sehen. Für den Auftraggeber stehen nur ausgewählte Ansichten zur Verfügung, bei denen die Daten eingeschränkt sind.

Daten werden an den jeweiligen Verantwortlichen mittels Datenbankschlüssel gebunden und Abfragen über die Rollen und Zugehörigkeitsdefinitionen durch die Applikation bestimmt. Damit sind abhängig vom Login die ersichtlichen Daten auf die zu dem systemseitig bestimmten Zweck und Auftraggeberbereich eingeschränkt.

Daten, die zum Zweck der Aufrechterhaltung und des reibungslosen Betriebs der Server und Applikationen dienen, sind nur Systemadministratoren der IT zugänglich.

Es gibt jeweils separate Datenbanken für Entwicklung und für das Produktivsystem.

Pseudonymisierung und Verschlüsselung

In CIRIS sind personenbezogene Daten, wie Accounts, mit den erforderlichen Daten über einen Schlüssel mit Aktivitätsdaten und Rollen verknüpft. Die Verbindung zwischen diesen Daten kann entweder das Programm oder ein Datenbankadministrator herstellen, beispielsweise um bestimmte Rollen und Berechtigungen zu vergeben und abzufragen. Im Klartext werden keine personenbezogenen Daten mit anderen Daten verknüpft und abgespeichert.

Dasselbe gilt nach Stand der Technik zum Verarbeiten von relationalen Datenbanken für das OTRS-System.

Eine Verschlüsselung der Daten findet nicht statt.

2. Integrität

Eingabekontrolle

Es wird lediglich das Datum der Anlage oder Änderung von Nutzerkonten protokolliert, nicht wer sie anlegt. Für die Anlage von Nutzerkonten ist der Verantwortliche beim Auftraggeber zuständig.

Bei der Anlage von Company Accounts werden die User ID und das Erstellungsdatum dokumentiert; zusätzlich wird das Datum der Änderung oder Löschung solcher Konten dokumentiert. Der erste Account des Auftraggebers ist ein Company Account, den die Administratoren von CIRIS anlegen. Jede weitere Anlage geschieht durch den Auftraggeber selber bzw. im Auftrag des Auftraggebers.

Company- oder Nutzerdaten können nicht direkt über CIRIS gelöscht werden. Vielmehr werden die Daten mit einer „Lösch“-Markierung versehen und sind damit für Anwender nicht mehr sichtbar. Eine endgültige Löschung bzw. Anonymisierung muss durch Datenbankadministratoren erfolgen.

Änderungen in Aktivitätsdaten mit personenbezogenen Daten sind programmtechnisch nicht möglich.

Änderungen direkt auf Datenbankebene mittels Umgehung der Applikation CIRIS werden systemseitig nicht protokolliert und sollen auch nicht stattfinden, es sei denn zur Korrektur von fehlerhaften Daten. Änderungen dieser Art, wie z.B. Löschung bzw. Anonymisierung von personenbezogenen Daten, werden auf Anfrage durchgeführt und sind damit innerhalb des Ticketsystems oder Projekttools dokumentiert.

Die Änderung bzw. Anlage von Company Accounts wird so lange gespeichert, bis die vertraglichen bzw. gesetzlichen Regelungen dies nicht mehr erfordern und die Daten entweder gelöscht oder anonymisiert werden, so dass keine personenbezogenen Daten mehr vorliegen.

Zugriff auf die Daten haben nur Mitarbeiter des Auftragnehmers, die auch Zugang zu der Datenbank bzw. Auswertungen über Qlikview davon haben. Der direkte Zugang zur Datenbank oder Auswertungen davon sind über die allgemeinen TOMs des Auftragnehmers geregelt.

Weitergabekontrolle

Anfragen für Anlage eines Company Accounts erfolgen über E-Mail an das Ticketsystem OTRS. Schutz der Daten ist gemäß den allgemeinen TOMs des Auftragnehmers gewährleistet.

Weitere personenbezogene Daten werden direkt in das System eingegeben und sind bezüglich Eingabe und Speicherung über die Applikationsrichtlinien und allgemeinen TOMs des Auftragnehmers gesichert.

3. Verfügbarkeit und Belastbarkeit

Alle Dienste laufen auf virtuellen Maschinen, die täglich gesichert werden. Im Falle eines Systemausfalls kann die virtuelle Maschine im Normallfall innerhalb von 10 Minuten zurückgesichert werden. Die Hardware läuft bei einem professionellen Hoster, der für den Auftragnehmer dedizierte ESX-Maschinen betreibt. Über Serviceverträge ist selbst bei komplettem Hardware-Ausfall eine Wiederaufnahme des Betriebes innerhalb eines Arbeitstages möglich.

Der Hoster unterliegt verschiedenen Zertifikaten zur Sicherheit und Verfügbarkeit von Daten – siehe auch Unterauftragnehmer Noris in **Anlage 2.**

Zertifikate:

ISO/IEC 27001: Informationssicherheitsmanagementsystem

ISO 27001: Zertifizierung auf der Basis von IT-Grundschutz

ISO/IEC 20000-1: Servicemanagementsystem

ISO 9001: Qualitätsmanagementsystem

VdS 3406: Objektspezifisches Sicherheitsmanagementsystem

PCI DSS: Payment Card Industry Data Security Standard

ISAE 3402 Typ II: Internes Kontrollsystem auf der Basis von COBIT 5

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Zunächst sind Richtlinien zum Umgang mit Daten sowie zur Verwendung von Hard- und Software grundlegend im Arbeitsvertrag der Mitarbeiter des Auftragnehmers enthalten und die Gewährleistung von Vertraulichkeit und Sicherheit von Daten, die im Unternehmen allgemein verarbeitet werden, im Grundsatz definiert.

Der Auftragnehmer sorgt durch entsprechende Verlautbarungen per E-Mail bzw. über das regelmäßig stattfindende Jour Fixe und das daraus resultierende Protokoll, das an alle Mitarbeiter versendet wird, für die nötigen, sich im Laufe der Zeit ergebenden Konkretisierungen und Anpassungen der Leitlinien zum Umgang mit personenbezogenen Daten. Darüber hinaus wird im Rahmen von Mitarbeiterschulungen, die anlassbezogen bei wichtigen Änderungen bzw. standardmäßig mindestens einmal im Jahr stattfinden, darauf näher eingegangen, so dass die Mitarbeiter für Datenschutz sensibilisiert werden und die Informationssicherheit durch entsprechende Leitlinien zum Umgang mit Daten gewährleistet ist.

Ein Datenschutzbeauftragter wurde benannt.

Als Unternehmen, das im Bereich IT-Dienstleistungen tätig ist, setzt der Auftragnehmer dem Stand der Technik entsprechende, geeignete Software ein, um sowohl die Sicherheit, Verfügbarkeit und Vertraulichkeit der Daten zu maximieren, als auch die gebotene Menge an personenbezogenen Daten auf das notwendigste zu beschränken.

Die Mitarbeiter sind aufgefordert bei allen Fragen in Bezug auf Datenschutz den Datenschutzbeauftragten zu kontaktieren. Darüber hinaus gibt es eine E-Mail-Adresse, die von einem Mitarbeiter über das Ticketsystem betreut wird, über die Betroffene ihre Rechte wahrnehmen können und an die Anfragen dieser Art von den Mitarbeitern weitergeleitet werden sollen, so dass Anfragen zeitnah beantwortet können.

Im zentral gepflegten Verzeichnis von Verarbeitungstätigkeiten werden die Prozesse und verarbeiteten personenbezogenen Daten aktuell gehalten und um weitere Dokumente, wie allgemeine TOMs, ergänzt.