Zusatzvereinbarung Auftragsverarbeitung

zwischen

Hotel Aschaffenburger Hof

Frohsinnstraße 11

DE-63739 Aschaffenburg

(nachfolgend „Auftraggeber“)

und

TourOnline AG, Borsigstrasse 26, 73249 Wernau

(nachfolgend „Auftragnehmer“)

zum Vertrag über die Erbringung von Dienstleistungen des Auftragnehmers für den Auftraggeber im Zusammenhang mit dem Betrieb des Buchungssystems „DIRS21“ (nachfolgend „Hauptvertrag“)

1. Allgemeines

1.1. Diese Zusatzvereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag und den dazu dem Auftraggeber zur Verfügung gestellten Dokumentationsunterlagen für das Buchungssystem DIRS21 in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.
1.2. 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.
1.3. 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

3.1. 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. 4.5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
3.2. Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.
3.3. Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.
3.4. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
3.5. Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.
3.6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
3.7. 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.

4. Allgemeine Pflichten des Auftragnehmers

4.1. 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.
4.2. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU), des Europäischen Wirtschaftsraums (EWR) oder der Schweiz durchzuführen.
4.3. 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.
4.4. Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **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

5.1. 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.
5.2. Die Pflicht zur Benennung eines Datenschutzbeauftragten nach 5.1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu bestellen 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

6.1. 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.
6.2. 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.
6.3. 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 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 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.

7. Mitwirkungspflichten des Auftragnehmers

7.1. 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. 11 dieses Vertrages.
7.2. 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.
7.3. 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. Kontrollbefugnisse

8.1. 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 im erforderlichen Umfang zu kontrollieren.
8.2. Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle nach Ziffer 8.1.erforderlich ist.
8.3. Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne der Ziffer 8.1 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. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.
8.4. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.
8.5. 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.

9. Unterauftragsverhältnisse

9.1. Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Ziffer 9.2 genannten Voraussetzungen zulässig.
9.2. 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. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines

neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information"). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information" zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information" erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

9.3. Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

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

9.5. 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.

9.6. Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 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.

9.7. Nicht als Unterauftragsverhältnisse im Sinne der vorstehenden Ziffern 9.1 bis 9.6 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-System 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.

10. Vertraulichkeitsverpflichtung

10.1. 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.

10.2. Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

10.3. Die Verpflichtung der Beschäftigten nach Ziffer 10.2 sind dem Auftraggeber auf Anfrage

nachzuweisen.

11. Wahrung von Betroffenenrechten

11.1. 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 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.
11.2. Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere 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.
11.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

12.1. 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.
12.2. 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.

13. Technische und organisatorische Maßnahmen zur Datensicherheit

13.1. 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.
13.2. 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 negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

14. Dauer des Auftrags

14.1. Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.
14.2. 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.

15. Beendigung

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.

16. Schlussbestimmungen

16.1. 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.
16.2. Für Nebenabreden ist die Schriftform erforderlich.
16.3. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den _____ Wernau, den 25.05.2019

Ort Datum

_____ _____

- Auftraggeber - - Auftragnehmer -

TourOnline AG
David Heidelberg –Vorsitzender des Vorstands-

Anlage 1 - Gegenstand des Auftrags

1. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Die im Zusammenhang mit der Buchung einer Unterkunft stehenden Daten, insbesondere Name und Anschrift des Buchenden, Name und Anschrift des Reisenden, Telefon, Email des Buchenden, An- und Abreisedatum, Anreisezeit, gebuchte Leistungen, Zahlungsmittel, Bemerkungen zu einer Buchung,

2. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

Personen, die eine Buchung vornehmen und Personen, die im Rahmen der getätigten Buchung anreisen

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(s) Unternehmen:

- TourOnline Service GmbH, Borsigstraße 26, 73249 Wernau, Deutschland
  Telefon: +49 715392500, Fax: +49 715392500, E-Mail: info@touronline.ag
  PCI-konforme Verarbeitung und Speicherung von Kreditkartendaten

- Datatrans AG, Kreuzbühlstrasse 26, 8008 Zürich, Switzerland
  Telefon: +41 44 256 81 91, Fax: +41 44 256 81 98, E-Mail: info@datatrans.ch
  PCI-konforme Verarbeitung und Speicherung von Kreditkartendaten

Anlage 3 - Technische und organisatorische Maßnahmen des Auftragnehmers

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

Beschreibung der technischen und organisatorischen Maßnahmen

1. Allgemeine Maßnahmen

Erfüllt:	ja	nein	
Sind die Mitarbeiter auf das Datengeheimnis verpflichtet?	☒	☐	Bitte Verpflichtungsmuster beilegen.
Ist die Verpflichtung nachweisbar dokumentiert?	☒	☐	Wo und in welcher Form? *In den Personalakten in Papierform*
Werden die Mitarbeiter regelmäßig bezüglich der Anforderungen des Datenschutzes unterwiesen (z.B. durch Schulungen)?	☒	☐	*Es finden jährlich interne Schulungen statt. Neue Mitarbeiter werden innerhalb der ersten zwei Wochen geschult.*
Besteht ein Testat über eine gesetzeskonforme Umsetzung des Datenschutzes im Unternehmen?	☒	☐	Welche Stelle hat das Testat ausgestellt? Auf welcher Normengrundlage wurde das Testat ausgestellt? *Die TourOnline AG ist PCI-Compliant nach PCI-DSS-Standard, dieser Standard übertrifft in der überwiegender Zahl der Kriterien der DSGVO.* Beruht das Testat auf einem externen Audit? ☒Ja ☐ Nein *Durch die Adsigo AG, Ludwigsburg.* Wie lange ist das Zertifikat noch gültig? *28.02.2019, das Zertifikat ist online im DIRS21 office für jeden Kunden abrufbar*
Welche Unternehmensbereiche umfasst das Zertifikat?			Bitte Kopie beifügen. *Alle Unternehmensbereiche, der „Report on Compliance" kann bei der TourOnline AG angefordert werden.*
Gibt es ein Datenschutzkonzept bzw. ein Datenschutzhandbuch zur Regelung und Umsetzung des Datenschutzes im Unternehmen?	☒	☐	Ist der Datenschutz ggf. durch andere Verfahrensanweisungen geregelt? ☐ Ja ☐ Nein Welche?
Wird die Datenverarbeitung auf dem Gebiet der Bundesrepublik Deutschland bzw. innerhalb der Europäischen Union	☒	☐	Ggf. in welchem Staat außerhalb dieses Gebiets?

oder der Staaten des Europäischen Wirtschaftsraums durchgeführt?			
Wird sichergestellt, dass für das Unternehmen tätige Unterauftrag-nehmer ebenfalls auf die Einhaltung der Vorschriften zum Datenschutz (DSVGO, BDSG, TKG, etc. verpflichtet werden?	☒	☐	☐Es findet keine Unterbeauftragung statt.

2. Technische und organisatorische Maßnahmen

☐ Die technischen und organisatorischen Maßnahmen werden im geforderten Umfang beschrieben. Das Ausfüllen der Anlage entfällt daher an dieser Stelle.

☒ Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen werden verbindlich zwischen Auftragnehmer und Auftraggeber festgelegt:

2.1 Zutrittskontrolle

Mit „Zutrittskontrolle" sind Maßnahmen gemeint, die einen unbefugten Zutritt zu Datenverarbeitungssystemen verhindern, mit denen personenbezogene Daten verarbeitet werden. Der Begriff ist räumlich zu verstehen.

☐ Das Kontrollziel **Zutrittskontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	**ja**	**nein**	
Besteht eine Regelung/Verfahren zur Besucherführung?	☒	☐	☒Empfang ☒ Besucherbuch ☒ Besucherausweis ☒ Persönliche Besucherführung ☐ Sonstiges:
Sind Zutrittssicherungen eingerichtet?	☒	☐	☒Zutrittskontrollsystem ☒ mit ☐ ohne Sicherheitszonen ☒ Zentrales Schließsystem ☒Sicherheitsschlösser ☐ Sonstiges: *Schließsystem/Zutrittskontrolle über RFID-Chips (Salto KS); im Rechenzentrum zusätzlich mit Fingerabdruck-Leser und Ausweis*
Sind sonstige Schutzmaßnahmen eingerichtet?	☒	☐	☐ Pförtner ☐ Wachdienst ☒ Alarmanlage ☐ Sonstiges *Die Alarmanlage ist zu einem Wachdienst aufgeschaltet, es liegt ein Alarmplan vor.*

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung:

2.2 Zugangskontrolle

Mit "Zugangskontrolle" sind Maßnahmen gemeint, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen oder gar entfernen oder schädigen. Im Gegensatz zur Zutrittskontrolle ist hier das Eindringen in das EDV-System von Seiten unbefugter Personen gemeint.

☐ Das Kontrollziel **Zugangskontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	ja	Nein	
Sind Maßnahmen zur Zugangskontrolle zum Desktop und zu den vernetzten Systemen eingerichtet?	☒	☐	☒Userkennung ☒Sicheres Passwort ☐ Passwortwiederholungssperre nach Fehlversuchen ☐ Andere Verfahren:
Bestehen für alle Zugriffsebenen (Netz, Server, Anwendungen) Passwortregeln zur Gewährleistung eines sicheren Passwortes?	☒	☐	
Wird die Einhaltung dieser Regeln auf allen Ebenen bei der Eingabe automatisiert kontrolliert?	☒	☐	*Im Active-Directory sind Anforderungen hinsichtlich der Mindest-Komplexität der Passwörter definiert.*
Ist eine zeitgesteuerte, passwort-geschützte Pausenschaltung (Bildschirmschoner) eingerichtet?	☐	☒	*Die Mitarbeiter sind verpflichtet ihren Rechner bei jedem Verlassen des Platzes zu sperren.*
Sind die vernetzten Systeme gegen unbefugtes Eindringen geschützt?	☒	☐	☒ Firewall ☒ Virenscanner ☐ Schnittstellenschutz (Netzwerkschaltschränke, Schutz nicht benötigter Netzwerksteckdosen etc.) In welcher Form? *Zum Einsatz kommen Router und Firewalls der Firmen Lancom und Juniper mit jeweils aktuellster Firmware.*
Bestehen sonstige Maßnahmen der Zugangskontrolle, z.B.?	☒	☐	☒Programmprüfungs- und FreigabeVerfahren ☒ Protokollierung und Auswertung von sicherheitskritischen Vorfällen ☐ Sonstige Maßnahmen:

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung:

2.3 Zugriffskontrolle

Mit „Zugriffskontrolle" sind Maßnahmen gemeint, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass bei der Bearbeitung der Daten diese nicht unbefugt gelesen, kopiert oder entfernt werden können. Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

☐ Das Kontrollziel **Zugriffskontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	**ja**	**nein**	
Besteht ein Berechtigungsprofil, das sicherstellt, dass jeder Mitarbeiter nur über die Zugriffsbefugnisse verfügt, die er zur Aufgabenerledigung benötigt?	☒	☐	In welcher Form? *Die Benutzer-Accounts erhalten je nach Team-/Abteilungszugehörigkeit individuelle Berechtigungen, die auf ihr Aufgabengebiet angepasst sind.* Soweit erforderlich auch differenziert nach ☒ Leseberechtigung ☒ Schreibberechtigung ☐ Sonstigen Berechtigungen, ggf. welche?
Sind die festgelegten Berechtigungen nachvollziehbar dokumentiert?	☒	☐	In welcher Form? *Nutzerprofil im Active-Directory*
Ist eine Rechteverwaltung eingerichtet, die bei einer Veränderung des Aufgabengebiets eine zeitnahe Aufhebung nicht mehr benötigter Rechte sicherstellt?	☒	☐	In welcher Form? *Checkliste im Personalwesen, die nach Änderung des Aufgabengebietes oder Ausscheiden des Mitarbeiters das Nutzerprofil anpasst bzw. deaktiviert.*

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung:

2.4 Weitergabekontrolle

Mit „Weitergabekontrolle" sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es dürfen in keinem Fall Datenträger oder Informationen verloren gehen.

☐ Das Kontrollziel **Weitergabekontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	ja	Nein	
Werden die Daten bei ihrer Übertragung vor unbefugter Kenntnisnahme geschützt?	☒	☐	☒Verschlüsselung ☐ Sichere Verbindungen, z.B. VPN ☐ Sonstige Maßnahmen:
Werden Datenübermittlungen nachvollziehbar protokolliert und kontrolliert?	☒	☐	Wie und in welcher Form? *Logfiles der Server*
Werden Schnittstellen von PCs und externe Laufwerke (mobile Festplatten, USB-Sticks etc.) gegen Missbrauch geschützt?	☒	☐	☐ Sperrung unbefugter Geräte ☐ Protokollierung der Nutzung ☐ Verschlüsselung der mobilen Datenträger ☒ Sicherheitsrichtlinien ☐ Sonstiges:
Ist die sichere Nutzung mobiler Datenträger geregelt?	☒	☐	Wie und in welcher Form? *Es dürfen keine privaten Datenträger genutzt werden und die firmeneigenen Datenträger müssen nach der Nutzung formatiert werden.*
Ist eine sichere Löschung/Entsorgung von Datenträgern gewährleistet?	☒	☐	Wie ist die Löschung/Entsorgung geregelt? *Die Entsorgung wird fachgerecht von der Firma Rhenus übernommen.*
Erfolgt bei Fernwartung der Zugriff auf die Kundendaten und Kundensysteme nur über sichere Leitungen?	☒	☐	Wie sind die Leitungen gesichert? ☒VPN ☒ Verschlüsselung ☐ Sonstiges: Ist dies auch bei einem Zugriff von anderen Stellen aus der Fall, z.B. im Home-Office? ☒Ja ☐ Nein *Verwendete Software: Lancom Advanced VPN Clients*
Ist bei Fernwartung eine sichere Identifizierung/Authentifizierung gewährleistet?	☒	☐	Bitte das Verfahren kurz beschreiben: *Die Fernwartung erfolgt ausschließlich durch eigene Mitarbeiter, deren Terminal identifiziert wird.*
Werden bei Fernwartung die Leitungen durch geeignete Sicherheits-einrichtungen (z.B. Protokollierung und	☐	☒	Art der Maßnahmen: *Nein, Fernwartungen durch externe Mitarbeiter*

Protokollauswertung) überwacht?	*oder Unternehmen sind untersagt, in dringenden Ausnahmefällen erfolgt die Wartung immer unter Aufsicht durch einen Mitarbeiter.*

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung:

2.5 Eingabekontrolle

Mit „Eingabekontrolle" sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

☐ Das Kontrollziel **Eingabekontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	**ja**	**Nein**	
Werden die Einwahlvorgänge in Kundensysteme nachvollziehbar protokolliert und überwacht?	☒	☐	In welcher Form? *Jeder Nutzer wird über seinen Login identifiziert.*
Werden die Benutzung von Datenverarbeitungssystemen und die Eingabe von Daten protokolliert?	☒	☐	Protokollierung der Dateibenutzung: ☒ Ja ☐ Nein Protokollierung von Eingaben und Veränderungen: ☐ Datenfeldbezogen ☒ Datensatzbezogen ☐ Dateibezogen ☐ Keine Protokollierung Die Protokollierung erfolgt auf Anwendungsebene

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung:

2.6 Auftragskontrolle

Mit „Auftragskontrolle" sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

☐ Das Kontrollziel **Auftragskontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	**ja**	**Nein**	
Wird die Durchführung des Kundenauftrags/der Serviceaktion nachvollziehbar überwacht, um eine auftragskonforme Erledigung zu gewährleisten?	☒	☐	In welcher Form? *Alle Daten werden ausschließlich zur Nutzung durch den Kunden freigegeben, von dem sie stammen. Alle anderen Anwendungsmöglichkeiten sind ausgeschlossen.*
Sind geeignete Protokollierungs- und Auswertungsmechanismen eingerichtet, um unzulässige Zugriffe auf Kundensysteme und Kundendaten zu überwachen?	☒	☐	In welcher Form? *Durch Protokollierungsfunktionen der Firewall-Systeme und Datenbank-Systeme.*

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung:

2.7 Verfügbarkeitskontrolle

Mit "Verfügbarkeitskontrolle" sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten vor aktiver (beabsichtigt destruktiver) und passiver (zufällig unbeabsichtigter) Zerstörung oder Veränderung, wie z.B. Hacking, Sabotage, Brand, Wasserschäden, Stromausfall etc. geschützt sind. Die vollständige Wiederherstellung des letzten Zustandes vor einem Verlustfall ist zu gewährleisten.

☐ Das Kontrollziel **Verfügbarkeitskontrolle** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	ja	Nein	
Sind die Kundendaten durch geeignete Sicherungsverfahren vor Zerstörung und Verlust geschützt?	☒	☐	z.B. ☒Gespiegelter Datenbestand ☒Regelmäßige Sicherungskopien/ Backup-Lösung ☐ Sonstiges: Gibt es ein Sicherungskonzept, in dem die Art und Weise einer regelmäßigen Sicherung und die Rekonstruktion der Daten festgelegt ist? ☒ Ja ☐ Nein
Werden die Sicherungsbestände sicher verwahrt?	☒	☐	In welcher Weise? *Physisch und logisch gesichertes NAS,*
Weitere vom Auftragnehmer umgesetzte Maßnahmen:			
Bemerkung:			

2.8 Trennungsgebot

Mit „Trennungskontrolle" sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung; eine logische Trennung der Datenträger ist ausreichend.

☐ Das Kontrollziel **Trennungsgebot** ist für die Auftragsdatenverarbeitung nicht umsetzbar oder relevant.
Begründung:

Erfüllt:	**ja**	**nein**	
Sind die Daten der verschiedenen Kunden in geeigneter Weise voneinander getrennt, um eine getrennte Verarbeitung zu gewährleisten?	☒	☐	Art der Trennung: Logische Trennung auf ☐ Betriebssystemebene ☐ Anwendungsebene ☒ Mandantentrennung ☐ Physikalische Trennung

Weitere vom Auftragnehmer umgesetzte Maßnahmen:

Bemerkung: