Auftragsverarbeitungsvereinbarung nach DSGVO der dtms GmbH

1. Allgemeines

1.1 Nachfolgende Bedingungen regeln das zwischen der dtms GmbH, Taunusstraße 57, 55118 Mainz (nachfolgend „dtms" oder „Auftragnehmer" genannt) und dem Vertragspartner (nachfolgend „Partner" oder „Auftraggeber" genannt) begründete Vertragsverhältnis hinsichtlich der Verarbeitung personenbezogener Daten durch dtms im Auftrag des Partners als Auftraggeber im Sinne des Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO).

1.2 Die Bestimmungen dieser Vereinbarung regeln die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten. Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1.3 Soweit dtms in Bezug auf die Verarbeitung personenbezogener Daten im Sinne von Art. 95 DSGVO besonderen in der Richtlinie 2002/58/EG bzw. der Datenschutzrichtlinie für elektronische Kommunikation festgelegten Pflichten unterliegt, werden dtms durch die DSGVO keine zusätzlichen Pflichten auferlegt, so dass dann eine Auftragsverarbeitungsvereinbarung nicht geboten ist; mithin kommt in diesen Fällen die Regelungen dieser Vereinbarung nicht zur Anwendung.

2. Gegenstand des Auftrags

2.1 Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Ziffer 19. festgelegt.

2.2. Die Daten fallen bei der Verwendung der in Ziffer 19. genannten Leistungen und/oder Produkte der dtms an, soweit der Partner ein Vertragsverhältnis über eine der dort bezeichneten Leistungen und/oder Produkte mit dtms eingegangen ist.

3. Rechte und Pflichten des Partners

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 Ziffer 4.6 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. Für Weisungen ist die Textform ausreichend.

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, werden diese dem Auftragnehmer mitgeteilt (Textform ausreichend). Für den Fall, dass sich die mitgeteilten weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer mindestens 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 von dtms

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 Auftragsverarbeiter 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) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

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

4.4 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.

4.5 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.

4.6 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.

4.7 Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden, werden diese dem Auftraggeber mitgeteilt (Textform ausreichend). Für den Fall, dass sich die mitgeteilten weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber mindestens in Textform mitteilen.

5. Datenschutzbeauftragter von dtms

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. Die Kontaktdaten vom Datenschutzbeauftragten des Auftragnehmers sind unter https://www.dtms.de/datenschutzhinweis/ einsehbar.

5.2 Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Ziffer 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 von dtms

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, 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, 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 von dtms

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 Ziffer 11.

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 jederzeit im erforderlichen Umfang zu kontrollieren.

8.2 Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle im Sinne von Ziffer 8.1 erforderlich ist.

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

8.4 Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne von 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.

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 Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Genehmigung des Auftraggebers in Textform zulässig, sofern bei Vertragsschluss ein solches Unterauftragsverhältnis nicht bereits bestand. Der Auftragnehmer wird alle bereits zum Vertragsschluss im Sinne von Ziffer 2.2 bestehenden Unterauftragsverhältnisse gemäß Ziffer 20.2 angeben.

9.2 Der Auftragnehmer hat 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.

9.3 Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. 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.

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 gemäß Ziffer 8. 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 i.S.d. 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 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. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

10.2 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.

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. Geheimhaltungsverpflichtung

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. Vergütung

Die Vergütung des Auftragnehmers richtet sich abschließend nach dem im Sinne von Ziffer 2.2 eingegangen Vertragsverhältnis über Leistungen und/oder Produkte der dtms, in dessen Rahmen die Datenverarbeitung vorgenommen wird.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

14.1 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.

14.2 Der zum Zeitpunkt des Vertragsschlusses im Sinne von Ziffer 2.2 bestehende Stand der technischen und organisatorischen Maßnahmen ergibt sich aus Ziffer 21. 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.

14.3 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.

15. Dauer des Auftrags

15.1 Die Dauer des Auftrages erstreckt sich über die Laufzeit des Vertragsverhältnisses im Sinne von Ziffer 2.2.

15.2 Der Auftraggeber kann die Vereinbarung über die Datenverarbeitung im Auftrag im Wege vorliegender Regelungen 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.

16. Beendigung

16.1 Nach Beendigung Vereinbarung über die Datenverarbeitung im Auftrag im Wege vorliegender Regelungen 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. Sofern unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der beiderseitigen Interessen der Parteien eine Löschung vorzuziehen ist, erfolgt keine Rückgabe in vorgenanntem Sinne. Eine Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

16.2 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.

17. 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.

18. Sonstige Bestimmungen

18.1 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.

18.2 Für Nebenabreden ist die Schriftform erforderlich.

19. Gegenstand und Zweck der Verarbeitung

19.1 Der Auftrag des Partners als Auftraggeber an die dtms als Auftragnehmer kann folgende Arbeiten, Leistungen und/oder Produkte umfassen:

a) DialogControl & digicom

Nachfolgendes gilt, sofern der Auftragnehmer für den Auftraggeber die Leistung DialogControl oder digicom erbringt. Dieses Anrufmanagementsystem umfasst die Funktionen des Call Routings und Monitorings von Anrufen zu Rufnummern des Auftraggebers. Hierzu zählen unter anderem

Routing-Optionen (z.B. Ursprung, Prozent, Tages-/Geschäftszeiten) und Warteschleifen-Funktionen (z.B. dynamisch oder fest, Priorisierung, Begrenzung), Call-Recording sowie derzeit elf Statistik-Arten.

- Routing-Optionen (z.B. Ursprung, Prozent, Tages-/Geschäftszeiten)
- Warteschleifen-Funktionen (z.B. dynamisch oder fest, Priorisierung, Begrenzung)
- Call-Recording
- sowie derzeit elf unterschiedliche Statistik-Arten (mit anonymisierten Teilnehmerdaten).

Über den Online-Monitor besteht die Möglichkeit, jederzeit alle Informationen über aktive Gespräche als auch wichtige Kennzahlen der Warteschleifen, Gruppen, der Agenten und Service-Rufnummern auf einen Blick einzusehen. Innerhalb des Anrufmanagementsystems werden die jeweiligen Anruferdaten in der Satistikart

- „Einzelverbindung" sowie den Features
- „Last Agent Routing",
- „Last Queue Routing",
- „Anrufhistorie" und
- „Adressbruch"

verwendet. In der über das Anrufmanagementsystem abrufbaren Satistikart „Einzelverbindung" werden die eingehenden und ausgehenden Anrufe des jeweiligen Teilnehmers samt dessen A-Rufnummer gespeichert. Das Anrufmanagementsystem kann anhand der A-Rufnummer abgleichen, ob innerhalb eines definierten Zeitraums (maximal 30 Tage) bereits ein

Anruf erfolgt ist. Im Feature „Last Agent Routing" kann einem auf diese Weise zuvor erfassten Teilnehmer anhand seiner A-Rufnummer der im vorherigen Anruf zugeteilte Agent erneut zugeteilt werden, sofern dieser zum Zeitpunkt des erneuten Anrufs im System angemeldet ist. Im Feature „Last Queue Routing" ist analog eine sofortige Weiterleitung in die Warteschleife des vorherigen Routingziels möglich. Im Feature „Anrufhistorie" wird dem bearbeitenden Agent für jeden eingehenden Anruf die bisherige Anrufhistorie anhand der A-Rufnummer über das Anrufmanagementsystem angezeigt. Im Feature „Adressbuch" können die Daten eines Anrufers gespeichert und im Falle eines erneuten Anrufs abgerufen werden. Diese Daten lassen sich auch für Outboundanrufe verwenden. Ein Call-Recording findet lediglich rein technisch über das Anrufmanagementsystem (Aufnahme und Erzeugung Voice-Files) statt. Die Daten werden an eine interne Lösung (idStorage) oder auf einen SFTP-Server des Kunden übermittelt und dort gespeichert. Ein Hosting und die Anzeige von Call-Recording-Daten erfolgt nicht über das Anrufmanagementsystem, sondern stets vom jeweiligen Speicherort aus. Im Übrigen wird auf die zusätzliche Leistungsbeschreibung verwiesen, welche in dem zwischen den Parteien geschlossenen Vertrag zur Erbringung des Anrufmanagementsystems festgehalten ist.

b) Multichannel ACD

Nachfolgendes gilt, sofern der Auftragnehmer für den Auftraggeber die Leistung Multichannel ACD erbringt. Die Leistung Multichannel ACD umfasst regelmäßig

- Ansagen abhängiges Routing,
- Zeitabhängiges Routing,
- Prozentrouting und
- Warteschleifen-Funktionen sowie
- IVR Menüs,
- Mailbox- und
- Call-Recordingoptionen.

Über den individuell konfigurierbaren Onlinemonitor besteht die Möglichkeit, dass der Auftraggeber stets einen aktuellen Überblick über Servicehotlines, Warteschleifen und Agentengruppen hat. Statistiken können hierbei online abgerufen oder automatisiert per E-Mail versandt werden. Ein abgestuftes Rechtemanagementermöglicht beliebig viele Logins mit individuell zugewiesenen Konfigurations-, Statistik- und Monitoringoptionen. Die Funktionalitäten der Multichannel ACD ermöglichen ferner das Routen eingehender Anrufe auf externe Kopfnummern und die Verteilung über lokale ACD Systeme oder den integrierten CTI Agentenclient, um Anrufe direkt auf verschiedene Endgerätezu verteilen. Der Agentenclient verfügt über einen Warteschleifenmonitor, erfasst beliebige Pausen- und Anrufgründe, zeigt Anruferdaten sowie Anrufhistorie. Die vorbezeichnete Call-Recordingoption sowie das einhergehende Screen-Recording lässt sich in der Multichannel ACD im Menü über die Module Aufnahmemodus und Black-/Whitelist ansteuern. In der Black-/Whitelist lassen sich die Anwendungen hinterlegen, die auf dem User-PC aufgezeichnet (Whitelist) bzw. nicht aufgezeichnet (Blacklist) werden dürfen, wobei sich je nach Bedarf einer oder mehrere Funktionsblöcke definieren lassen.

c) Gewinnspiel

Nachfolgendes gilt, sofern der Auftragnehmer für den Auftraggeber die Leistung Gewinnspiel erbringt. Im Falle der Leistung Gewinnspiel ist der Gegenstand und Zweck des Auftrages die Abwicklung eines Gewinnspiels oder einer Verlosung für den Auftraggeber auf einer Telekommunikationsplattform des Auftragnehmers. Die Teilnahme erfolgt per Telefon oder SMS. Der Aufragnehmer stellt dem Auftraggeber die Teilnehmerdaten zur Gewinnermittlung zur Verfügung. Ausdrücklich nicht umfasst sind die Maßnahmen Gewinner-Ermittlung, Gewinner-Benachrichtigung, Versand der Gewinne oder die Abwicklung eines Geldpreises. In Bezug auf Call-Recording bei Gewinnspielen siehe Ziffer 1. e).

d) idStorage

Nachfolgendes gilt, sofern der Auftragnehmer für den Auftraggeber die Leistung idStorage erbringt. Mit idStorage werden Daten, insbesondere Voice-Files, welche aus verschiedenen Anwendungen des Auftragnehmers (z.B. DialogControl) stammen können, gespeichert. Die Speicherung dieser Voice-Files erfolgt auf einem Dateiserver (NAS) des Auftragnehmers. Der Zugriff auf die Daten in idStorage bzw. der Login erfolgt durch den Kunden über ein https-verschlüsseltes WebFronted durch Eingabe nutzerindividueller Zugangsdaten. Nach dem Login kann der Kunde die Daten anhören und/oder downloaden. Innerhalb des Interfaces als auch den Dateibezeichnungen werden A-Rufnummern stets anonymisiert dargestellt. Sofern die vom Nutzer beauftragte Speicherkapazität in idStorage nicht mehr ausreicht, werden die jeweils ältesten Daten gelöscht.

e) Anrufaufzeichnung (Call-Recording)

Nachfolgendes gilt, sofern im Zusammenhang mit einer Leistung oder Anwendung des Auftragnehmers eine Anrufaufzeichnung (Call-Recording) für den Auftraggeber erfolgt. Neben dem Call-Recording über das Anrufmanagementsystem in idStorage oder in einem SFTP-Server des Kunden kann eine Anrufaufzeichnung noch bei Gewinnspielen (z.B. bei Nutzung von Online Gewinnerziehung) oder bei der Nutzung von WebControl Media erfolgen.

WebControl Media ist ein Online-Tool, um die vom Kunden genutzten Service-Rufnummern und IVR-Anwendungen konfigurieren, steuern oder auswerten zu können. Online Gewinnerziehung ist ein Online-Tool, um die Gewinner eines Gewinnspiels zu ermitteln. Die Speicherung von Voice-Files bei der Nutzung von WebControl Media oder Online Gewinnerziehung erfolgt auf einem Dateiserver (NAS) des Auftragnehmers. Der Login erfolgt durch den Kunden über ein https-verschlüsseltes WebFronted durch Eingabe nutzerindividueller Zugangsdaten. Nach dem Login kann der Kunde die Daten anhören und/oder downloaden, wobei bei der Gewinnerziehung eine zufällige Wiedergabe erfolgt.

Im Falle von IVR-Anwendungen, welche durch den Auftragnehmer kundenindividuell eingerichtet werden können, erfolgt die Bereitstellung der in der Anwendung erzeugten Voice-Files durch Speicherung auf einem SFTP-Server des Kunden, über einen telefonischen Abhördienst per zufälliger Wiedergabe von Voice-Files (z.B. Gewinnerziehung) oder als sogenannter Transkriptionsdienst (sequenzielles Abspielen). Ferner kann ein Zugriff über die vorbeschriebenen Online-Tools erfolgen.

Im Rahmen der Anrufaufzeichnung besteht die Möglichkeit zur Transkription der jeweiligen Aufnahmen (z.B. Adressdaten von Gewinnspielen). Die MitarbeiterInnen eines Dienstleisters transkribieren die Aufnahmen und senden die Abschriften an den Auftraggeber.

Innerhalb einer IVR-Anwendung werden A-Rufnummern stets anonymisiert dargestellt.

f) Call-Center-Leistung

Nachfolgendes gilt, sofern der Auftragnehmer dem Auftraggeber auch die Nutzung eines Call-Centers bereitstellt, z.B. im Rahmen der Leistung Auskunft 118xy oder im Entertainmentbereich, wobei die Call-Centerleistung nicht durch den Auftragnehmer selbst erbracht wird. Der Auftragnehmer ist nicht Betreiber eines Call-Centers und auch nicht gesellschaftlich an dem jeweilig genutzten Call-Center beteiligt. Der Auftraggeber nutzt dieses – durch den Auftragnehmer bereitgestellte und durch einen Dritten betriebene – Call-Center zur Erbringung von Entertainmentleistungen (z.B. Erotik, Astrologie und/oder zur Beauskunftung seiner Teilnehmer, welche bei seiner Auskunftsrufnummer der Rufnummerngasse 118xy anrufen. Eine zusätzliche Leistungsbeschreibung in Bezug auf die konkrete Leistung ist in dem zwischen den Parteien geschlossenen Vertrag zur Erbringung von Call-Center-Leistungen festgehalten.

- Auskunft 118xy:

Der Auftragnehmer erbringt für den Auftraggeber in seinem Namen Auskunftsdienstleistungen. Zu diesem Zweck werden auf den vertraglich vereinbarten Auskunftsnummern eingehende Anrufe an den Auftragnehmer weitergeleitet. Den Anrufern wird von den Mitarbeitern des Auftraggebers vornehmlich Auskunft über die Telefonnummer einer vom Anrufer genannten Person u./ o. Firma gegeben. Zudem besteht die grundsätzliche Möglichkeit der Verbindung zu Sonderzielen auf Wunsch des Anrufers.

- Entertainmentdienste:

Im Erotikbereich können über das Callcenter ein moderierter Adult-Entertainment-Dienst erreicht werden, indem die Operatoren im Callcenter die geäußerten Vorlieben von Anrufern entgegennehmen und nach Ermittlung einer dazu passenden Gesprächspartnerin eine Weitervermittlung an diese vornehmen. Ferner existiert die Möglichkeit, dass Anrufer sich die Profilaufsprachen von potentiellen Gesprächspartnerinne anhören und sich

automatisiert per Tastendruck an diese weitervermitteln lassen.

Im Falle von Astrologiediensten hören die Anrufer die Profilaufsprachen von BeraterInnen und können sich automatisiert per Tastendruck an diese weitervermitteln lassen, um eine Lebensberatung per Telefon zu erhalten. Ferner besteht für Anrufer die Möglichkeit sich direkt an eine/n BeraterInnen über die Eingabe einer PIN vermitteln zu lassen. Diese PIN wurde vorab beispielsweise über eine Webseite oder durch die BeraterInnen in einem vorherigen Gespräch kommuniziert, so dass eine direkte Verbindung hergestellt werden kann.

Die vorgenannten Entertainmentdienste werden hauptsächlich über 0900er-Rufnummern (Premium-Dienste i.S.d. § 3 Nr. 17c TKG), Premium-Voice Rufnummern (Kurzwahldienste i.S.d. § 3 Nr. 11b TKG) oder Keywords auf 118xy-Rufnummern (Auskunftsdienste i.S.d. § 3 Nr. 2a TKG) erbracht. Möglich ist auch ein Einsatz deutschsprachiger Entertainmentdienste auf einer ausländischen Premium-Dienste-Rufnummer.

g) Transkriptionsleistungen

dtms bedient sich im Falle von Anrufaufzeichnungen für die Transkription eines Unterauftragnehmers. Diese Leistung ist optional vom Auftraggeber buchbar.

h) PeakControl

PeakControl ist eine IVR Anwendung mit dazugehörigem Online Tool. Die IVR Anwendung wird als Überlaufziel einer ACD Anwendung angesteuert, sofern keine angemeldeten Contact Center Agenten verfügbar sind. Dem Anrufer wir über PeakControl ein Rückruf durch das Contact Center angeboten. Hierbei wird er aufgefordert seine vollständige A-Nummer einzugeben. Sofern die vollständige A-Nummer bereits übermittelt wurde, wird er gebeten, sein Einverständnis zur Rückruf-Nutzung zu geben. In beiden Fällen wird die A-Nummer auf dem IVR System gespeichert.

Der Zugriff bzw. Login auf das Online Tool „Peak Control" erfolgt durch den dtms Kunden über ein https-verschlüsseltes Web-Fronted durch Eingabe nutzerindividueller Zugangsdaten. Nach dem Login kann der Kunde über den Menüpunkt „Rückruf-Monitor" alle für ihn vom Peak-Control System ausgeführten Rückrufe einsehen. Hierbei wird u.a. die vollständige A-Nummer (zwecks Kontaktaufnahme bei z.B. misslungenen Verbindungsversuchen) ausgegeben.

i) Kunden-Feedback

Kunden Feedback ist eine IVR Anwendung mit dazugehörigem Online Tool. Die IVR Anwendung dient zur telefonischen Abfrage von Kundenbewertungen zu vom dtms Kunden definierten Fragen. Hierbei kann bei bestimmten Frage/Antwort Konstellationen eine angekündigte, freiwillige Aufsprache durch den Anrufer erfolgen (Freie Meinung hinterlassen). Die Kundenbewertung sowie das Audio (sofern eines aufgezeichnet wurde) werden dem dtms Kunden über das Online Tool „Kunden-Feedback" bereitgestellt. Hierbei wird ebenfalls die A-Nummer (anonymisiert, sofern der Anrufer Rufnummernunterdrückung aktiviert hat) bereitgestellt.

Der Zugriff bzw. Login auf das Online Tool „Kunden-Feedback" erfolgt durch den dtms Kunden über ein https-verschlüsseltes Web-Fronted durch Eingabe nutzerindividueller Zugangsdaten.

j) WebControl Media

WebControl Media ist eine IVR Anwendung mit dazugehörigem Online Tool. Über das Online Tool können durch den dtms Kunden Telefon-Gewinnspiele (für seine Service-Rufnummern) auf IVR Basis konfiguriert und aktiviert werden. In diesem Zusammenhang können bei Gewinnspielen Aufsprache Audios generiert werden, z.B. wenn Anrufer / Teilnehmer Namen und Adresse zwecks Gewinnbenachrichtigung hinterlassen. Diese Audios können über das Online Tool „WebControl Media" durch den dtms Kunden (zwecks Gewinnbenachrichtigung) angehört und heruntergeladen werden. Die vollständige A-Nummer wird nur übertragen und gespeichert, sofern diese seitens des A-Teilnehmers übermittelt wurde.

Der Zugriff bzw. Login auf das Online Tool „WebControl Media" erfolgt durch den dtms Kunden über ein https-verschlüsseltes Web-Fronted durch Eingabe nutzerindividueller Zugangsdaten.

k) Click2Call

Click2Call ist eine IVR Anwendung bei der Teilnehmer auf einer Webseite des dtms Kunden über ein WebWidget (Webseiten-Plugin) einen Rückruf anfordern können. Hierbei ist die Eingabe der vollständigen A-Nummer (zwecks Rückruf) einzugeben. Die IVR Anwendung initiiert nach Eingabe der Rückrufnummer und Rückruf-Aufforderung durch den A-Teilnehmer einen Rufaufbau zum Contact Center (des dtms Kunden) sowie zum A-Teilnehmer.

l) Junk-Call Protection

Junk-Call Protection ist eine IN Anwendung bei der dtms Kunden eine sog. Blacklist für ihre Service-Rufnummern pflegen können. Hierbei wird durch Eingabe bestimmter Ziffern auf der Telefontatstatur des B-Teilnehmers (z.B. das Contact Center des dtms Kunden) die übermittelte A-Nummer des Anrufers für einen bestimmten Zeitraum (max. 7 Tage) im Intelligenten Netz (IN) der dtms gesperrt. Dies gilt zur Vermeidung von unerwünschten Anrufen (Junk-Calls) z.B. bei Freephone Rufnummern.

m) SMS- und Fax-Versand

Der Auftraggeber liefert dem Auftragnehmer Rufnummernlisten, an die ein SMS- oder Fax-Versand erfolgen soll, nebst weiterer Versandinformationen (Bulk/Massenversand). Sofern ein Versand von Werbung erfolgt, obliegt es dem Auftraggeber, die gesetzlich erforderliche Einwilligung des Teilnehmers einzuholen und zu dokumentieren. Der Auftraggeber unternimmt lediglich den technischen Versand sowie eine dahingehende Auswertung.

n) Beratung & Entwicklung

Bei der Leistung Beratung und Entwicklung handelt es sich um eine individuelle Leistung des Auftragnehmers, welche sich aus der Leistungsbeschreibung des jeweils geschlossenen Vertrages ergibt. Sofern bei dieser Leistung eine Verarbeitung personenbezogener Daten stattfindet und Ziffer 1.3 nicht zur Anwendung kommt, gelten ebenfalls die Regelungen dieses Vertrages.

19.2 Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- TKG-Daten (Bestands-, Verkehrs-, Standort- und Nutzungsdaten, Einzelverbindungsdaten im Sinne des Telekommunikationsgesetzes (TKG)
- Kommunikationsdaten (z.B. CDR-Daten, Telefondaten)
- Planungs- und Steuerungsdaten, welche mit dem Telekommunikationsrouting zusammenhängen
- Daten aus Kundenfeedback inklusive zugehöriger Sprachdaten (z.B. Voice-Files)
- Auskünfte
- Gesprächshistorie
- Abrechnungsdaten
- Leistungs-, Adress- und Kundendaten

19.3 Folgender Kreis der von der Datenverarbeitung betroffenen Personen liegt regelmäßig vor:

- Mitarbeiter/innen
- Interessenten/innen
- Kontaktpersonen
- Gesellschafter/innen
- Kunden/innen
- Teilnehmer gemäß § 3 Nr. 20 TKG
- Lieferanten/innen

20. Unterauftragnehmer

20.1 Der Auftragsnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer").

20.2 Die relevanten Unterauftragnehmer für die Leistungen und/oder Produkte, über welche ein Vertragsverhältnis im Sinne von Ziffer 2.2 besteht, werden dem Auftraggeber auf Anforderung mitgeteilt (Textform ausreichend).

20.3 Der Auftragnehmer und der jeweilige Unterauftragnehmer haben einen Vertrag über die Verarbeitung von Daten im Auftrag gemäß Art. 4 Nr. 8 und Art. 28 DSGVO geschlossen. Auf diese Vereinbarung wird im Hinblick auf die Datenverarbeitung im Auftrag im Unterverhältnis verwiesen.

21. Technische und organisatorische Maßnahmen (TOMs) der dtms

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

21.2 Zur Wahrung der Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DSGVO ergreift der Auftragnehmer folgende Maßnahmen:

a) Zutrittskontrolle

Der Auftragnehmer verwehrt unbefugten Zutritt zu den Büro-, Server- und Archivräumen. Dies geschieht durch:

- Zutrittskontrollsystem/ Zutritt nur für autorisierte Mitarbeiter mittels eines so genannten „Batch" und jeweils un-

ter Beachtung nachfolgender Grundsätze: Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen über ihre Identität und Anschrift, in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten, darüber, wie er seine Rechte ausüben kann, und über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

- Rücknahme von Zugangsmittel (Batch) erfolgt nach Ablauf der Berechtigung und wird von einem Mitarbeiter/einer Mitarbeiterin des Vertriebsinnendienstes schriftlich nachgehalten.
- Die Türsicherung erfolgt in Bonn und Hamburg in den Geschäftsräumen mittels eines Sicherheitsschlosses.
- Die Einlasskontrolle erfolgt jeweils am Empfang durch persönliche Kontrolle. Fremde Besucher haben sich einzutragen und werden bei den Besuchen persönlich zu den betreffenden Räumen begleitet. Sofern in den Räumen datenschutzrelevante Informationen einsehbar sind, erfolgt eine persönliche Begleitung des Besuchers.
- Im Alarmfall ist das Gebäude unverzüglich von allen Mitarbeitern zu verlassen. Die Türen sind sowohl in den Büroräumen, als auch in den Rechenzentren selbstschließend, so dass auch nach Verlassen der Räume sichergestellt ist, dass kein unberechtigter Zutritt durch Dritte erfolgen kann.
- Der Zutritt zum Gebäude ist durch Türschlösser gesichert und zusätzlich durch ein so genanntes Batch-System (elektronischer Eingangschip). Die Überwachungseinrichtung der Rechenzentren verfügt ferner über eine Alarmanlage und Videoüberwachung (24/7). Der Remotezugriff auf die Rechenzentren ist nur ausgewählten Mitarbeiter der Technik gestattet, welche mittels eines gesondert gesicherten virtuellen VPN-Tunnelzugriffs auf die Rechenzentren zugreifen können.

b) Zugangskontrolle

Der Auftragnehmer verhindert, dass EDV-Systeme von Unbefugten genutzt werden können. Dies geschieht durch:

- Es wird ein Kennwortverfahren angewendet (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), mit welchem sichergestellt wird, dass Passwörter die Mindestanforderungen an die Sicherheit erfüllen. Die Erteilung erfolgt für den IT-Bereich (PC, Drucker, sonstige Hardwareumgebung für die Office-IT durch die Schwestergesellschaft in Berlin – nexnet GmbH, dort durch den Leiter der IT-Abteilung). Für den TK-Bereich erfolgt die Erteilung durch den Leiter der Technik in Hamburg).
- Die Passwörter unterliegen genauen Sicherheitsvorgaben. Die Einzelheiten regelt die Passwort-Richtlinie der dtms GmbH (z.B. Mindestlänge 8 Zeichen, deren Einhaltung technisch überprüft und erzwungen wird). Ferner wird sichergestellt, dass nur Mitarbeiter der dtms GmbH zu den Bereich Zugriff erhalten, welche für ihre Arbeit erforderlich sind. Diese wird durch eine entsprechende Rechtevergabe in der Office-IT und im TK-Bereich sichergestellt.
- Ein Passwortwechsel wird alle 3 Monate erzwungen, indem der Mitarbeiter aufgefordert wird, sein Passwort zu ändern. Erfolgt dies nach wiederholter Aufforderung nicht, wird der Zugang gesperrt.
- Ebenso werden externe USB-Schnittstellen gesperrt und nur für Mitarbeiter freigeschaltet, die aufgrund ihrer beruflichen Tätigkeit dieses Medium benötigen. Der Umgang mit mobilen Geräten ist im Detail in der Richtlinie für mobile Geräte der dtms GmbH geregelt. Personenbezogene Daten dürfen auf mobilen Datenträgern nicht gespeichert werden.
- Die IT-Systeme im Bereich der Office-IT und im Bereich der Telekommunikation sind mittels einer Firewall vor Viren und Schadsoftware geschützt. Hierdurch werden unberechtigte Zugriffe erkannt und entsprechend unterbunden. Im Bereich des E-Mail-Zugangs werden die eingehenden E-Mails auf Viren und Schadsoftware geprüft und erforderlichenfalls in einem Quarantäne-Bereich abgelegt.
- Neben der vorstehend beschriebenen Firewall und dem Virenscanner verfügt die dtms GmbH zusätzlich noch über einen so genannten Schnittstellenschutz
- Es erfolgt die Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen.
- Die PC im Bereich der IT- und TK sind durch automatische, passwortgeschützte Bildschirm- und Rechnersperre gesichert
- Es erfolgt eine eindeutige Zuordnung von Benutzerkonten zu den Benutzern
- Sensible Systeme, insbesondere Serversysteme sind nur als Administrator nutzbar
- Die Übertragung von personenbezogenen Daten erfolgt nur im Netzwerk der Unternehmung (SSH, VPN) und somit gesichert.
- Der Zugriff auf das firmeninterne VPN ist nur über zertifikatsbasierte Authentifizierung möglich. Die Vergabe der Authentifizierungen ist in der IT-Richtlinie der dtms GmbH geregelt.
- Die Vernichtung von nicht mehr erforderlichen Datenträgern erfolgt mittels kontrollierter Vernichtung durch ein qualifiziertes Entsorgungsunternehmen
- Bei Ausscheiden eines Mitarbeiters/einer Mitarbeiterin hat der/die Betroffene alle Zugangsberechtigungen unverzüglich mit Ausscheiden zurückzugeben.

c) Zugriffskontrolle

Der Auftragnehmer gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

- Die Office-IT stellt nach Vorgabe der Geschäftsführung sicher, dass eine differenzierte Berechtigung (z.B. in Form von Profilen, Rollen, Transaktionen, Objekten) erteilt wird. Die Mitarbeiter haben nur Zugriff auf Bereich innerhalb der IT, welche für ihre jeweilige Tätigkeit erforderlich und geboten sind. Diese Berechtigungen werden jeweils zyklisch einer Kontrolle unterzogen. Die genauen Vorgaben regelt die IT-Richtlinie der dtms GmbH.
- Die Auswertungen, Kenntnisnahme, Veränderung, Löschung von personenbezogenen Daten erfolgen kontrolliert und werden protokolliert
- Es erfolgt eine automatische Sperre auf IT-Systeme, sofern eine mehrmalige fehlerhafte Authentifizierung vorgenommen wurde
- Vermeidung der Konzentration von Funktionen – Funktionstrennung von Administratorentätigkeit auf unterschiedliche qualifizierte Personen
- Bei Ausscheiden eines Mitarbeiters/einer Mitarbeiterin hat der/die Betroffene werden alle Zugangsberechtigungen unverzüglich mit Ausscheiden gesperrt.

d) Trennungskontrolle

Der Auftragnehmer gewährleistet, 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. Dies geschieht durch:

- Sofern Daten zu verschiedenen Zwecken verarbeitet werden, wird sichergestellt, dass die Verarbeitung jeweils nur mandantenbezogen für den/die jeweils betroffene Person erfolgt. Die Systeme für die Endkundenbearbeitung verfügen über eine interne Mandantenfähigkeit und richten sich nach dem jeweiligen Zweck der Verarbeitung der personenbezogenen Daten (Zweckbindung)
- Funktionstrennung / Produktion / Test
- Logische Trennung personenbezogener Daten verschiedener Auftraggeber
- Kennzeichnung erfasster Daten (Aktenzeichen, CRM- und Abrechnungsnummer)

e) Pseudonymisierung

In Bezug auf bestimmte personenbezogene Daten erfolgt statt einer Löschung die Anonymisierung der Daten, so dass die

Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

21.3 Zur Wahrung der Integrität gemäß Art. 32 Abs. 1 lit. b DSGVO ergreift der Auftragnehmer folgende Maßnahmen:

a) Eingabekontrolle

Der Auftragnehmer gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Die Eingabe wer Daten in die Systeme eingibt erfolgt durch Protokollierungs- und Protokollauswertungssysteme. In sensiblen Bereichen ist erkennbar von welchem PC mit welcher Zugriffsberechtigung die Daten eingegeben, geändert oder gelöscht wurden. Zugriff auf die jeweiligen Protokollen haben für den Bereich der Office-IT der Leiter der Office-IT und dessen Stellvertreter/in und die Geschäftsführer, für den Bereich der in der Telekommunikation verwendeten IT der/die Leiter/in Technik und deren/dessen Stellvertreter sowie die Geschäftsführer.
- Sowohl im Bereich der Office-IT als auch im Telekommunikationsbereich gilt das Berechtigungskonzept der dtms GmbH (IT-Richtlinie der dtms GmbH)
- Durch das Berechtigungskonzept ist sichergestellt, dass der Zugriff von Mitarbeitern auf erforderliche Daten nur im Rahmen seiner jeweiligen Funktion im Unternehmen erfolgt und nur in dem Umfang, die für seine Tätigkeit im Unternehmen erforderlich und geboten ist.
- Berechtigungsvergaben auf schützenswerte Ressourcen werden nachvollziehbar nur durch hierfür autorisierte Personen beantragt und vergeben

b) Weitergabekontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Es erfolgt eine Verschlüsselung bei der Datenübertragung mittels SSH oder SSL bzw.je nach Anwendung auch durch eine Tunnelverbindung (VPN = Virtual Private Network)
- Die Schnittstellen von PCs sind vor dem Zugriff und der Koppelung durch unbefugte nicht autorisierte Hardware und andere technische Geräte geschützt.
- Bei dem Datenaustausch wird die Übertragung standardmäßig mittels Transportprotokolle (SSL) gesichert.
- Im Falle von Heimarbeit wird die Datenübertragung im vorgenannten Sinne verschlüsselt; eine Übertragung von Daten ist ausschließlich durch eine Tunnelverbindung möglich
- Die datenschutzgerechte Entsorgung von Papier- und Datenträger erfolgt durch ein hierfür qualifiziertes Unternehmen

21.4 Zur Wahrung der Verfügbarkeit und Belastbarkeit gemäß Art. 32 Abs. 1 lit. b DSGVO ergreift der Auftragnehmer folgende Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.:

- Backup-Verfahren / regelmäßige Sicherungskopien
- Überwachung der Computersysteme
- Einsatz von unterbrechungsfreier Stromversorgung (USV) und Notstromaggregaten im Rechenzentrum. Vorhandensein von Klima- und Brandmeldeanlage sowie Überspannungsfilter
- Getrennte Aufbewahrung
- Ständig aktualisierte/r Virenschutz/Firewall
- Notfallplan
- Rasche Wiederherstellbarkeit durch vollständige Redundanz der Rechenzentrumsstandorte.
- Die Standorte der Rechenzentren des Auftragnehmers lauten wie folgt:

  Wendenstr. 408, 20537 Hamburg und Reuchlinstr. 10/11, 10553 Berlin

21.5 Das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gemäß Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO gestaltet sich wie folgt:

- Die Unternehmensleitung hat Leitlinien zum für Datenschutz und die Informationssicherheit erlassen und im Intranet für die Mitarbeiter veröffentlicht. Es gibt ferner Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten. Die Beschäftigten werden regelmäßig, mindestens einmal im Kalenderjahr, zum Datenschutz geschult. Die Beschäftigten werden durch ihren zum vertraulichen Umgang mit personenbezogenen Daten und auf das Fernmeldegeheimnis durch ihren Arbeitsvertrag verpflichtet. Diese werden zudem auf ihre Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse hingewiesen. Im Unternehmen des Auftragnehmers gilt das Vier-Augen-Prinzip.
- Technische Maßnahmen zur Umsetzung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) sind nicht gesondert getroffen, da das TKG diesbezüglich abschließende und restriktivere Regelungen in Bezug auf den Umgang mit Bestands- und Verkehrsdaten trifft.
- Anfragen von Betroffenen werden an einen für diesen Zweck vorgesehenen Mitarbeiter weitergeleitet, der diese Anfragen zeitnah bearbeitet und mit dem Datenschutzbeauftragten koordiniert.
- Der Auftragnehmer hat ein Datenschutzmanagementsystem (DSMS) implementiert. Durch ein Fraud-Management-System wird sichergestellt, dass Datenschutzverletzungen erkannt und unverzüglich gemeldet werden. Der Auftragnehmer verfügt für ihre Prozesse im Rahmen derer personenbezogene Daten verarbeitet werden über entsprechende Verzeichnisse von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO.
- Die Auftragsverarbeitung im Sinne von Art. 28 DS-GVO erfolgt entsprechend den Weisungen des Auftraggebers und zur Erfüllung des vertraglich definierten Verwendungszweckes. Eine Verarbeitung der Daten erfolgt in der Europäischen Union und im Europäischen Wirtschaftsraum.