

Vertrag über die Auftragsverarbeitung personenbezogener Daten nach Art. 28 Datenschutz-Grundverordnung (DSGVO)

Der Auftragsverarbeiter:

myhotelshop GmbH
Floßplatz 6
04107 Leipzig
(im Folgenden "MHS")

Präambel

Der Kunde nutzt die von MHS angebotenen Dienste, um das Direktgeschäft von Hotels nachhaltig zu steigern.

In diesem Zusammenhang ist nicht ausgeschlossen, dass der Kunde personenbezogene Daten verarbeitet. Nach Art. 28 DSGVO ist hierfür der Abschluss eines Auftragsdatenverarbeitungsvertrags erforderlich.

Voraussetzung für die Zulässigkeit einer solchen Auftragsverarbeitung i.S.d. Art. 28 DSGVO ist, dass der Kunde MHS den Auftrag erteilt. Dieser Vertrag enthält diesen Auftrag des Kunden an MHS und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Datenverarbeitung sowie die sich daraus ergebenden besonderen Pflichten in Bezug auf Datenschutz und Datensicherheit. Grundsätzlich ist der Kunde für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz verantwortlich und behält insofern die Herrschaft über die zu verarbeitenden Daten. Im Folgenden wird für den Kunden der Begriff des "Verantwortlichen" genutzt.

1. Allgemeines

a) MHS verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU)2016/679 – Datenschutzgrundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

b) 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

Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem zugrundeliegenden Auftrag in Zusammenhang stehen und bei denen Mitarbeiter von MHS oder durch MHS beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen oder durch Bereitstellung des Verantwortlichen in Berührung kommen können. Der Auftrag des Verantwortlichen an MHS umfasst die in der **Anlage 1** wiedergegebenen Arbeiten und/oder Leistungen. Aus der Anlage ergibt sich zudem der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen.

3. Pflichten von MHS

a) MHS verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Verantwortlichen erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die MHS ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt MHS dem Verantwortlichen 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 Verantwortlichen. Eine hiervon abweichende

Verarbeitung von Daten ist MHS untersagt, es sei denn, dass der Verantwortliche dieser schriftlich zugestimmt hat.

b) MHS verpflichtet sich, die Datenverarbeitung im Auftrag, in der Regel, nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

c) Jede Verlagerung der Datenverarbeitung oder Nutzung in ein Drittland bedarf der Genehmigung des Auftraggebers und darf nur erfolgen, wenn die gesetzlichen Regelungen, nach den §§ 78 ff. BDSG, ebenso Art. 44 und Art. 49 DSGVO, eingehalten werden. Dies betrifft unter anderem die Auftragserteilung, welche die Nutzung von Unterstützungsplattformen erfordert. In **Anlage 1** verweist MHS auf die jeweils geltenden Datenschutzerklärungen. Die Genehmigung gilt als erteilt, wenn dem Auftragsdatenverarbeitungsvertrag zugestimmt wird und die Nutzung der Unterstützungsplattformen in die Verarbeitung mit einfließt.

d) MHS wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. MHS ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Sofern MHS darlegen kann, dass eine Verarbeitung nach Weisung des Verantwortlichen zu einer Haftung von MHS nach Art. 82 DSGVO führen kann, steht MHS das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

4. Meldepflichten von MHS

a) MHS ist verpflichtet, dem Verantwortlichen jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Verantwortlichen, 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 MHS im Auftrag des Verantwortlichen verarbeitet.

b) Ferner wird MHS den Verantwortlichen unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber MHS tätig wird und dies auch eine Kontrolle der Verarbeitung, die MHS im Auftrag des Verantwortlichen erbringt, betreffen kann.

c) MHS ist bekannt, dass für den Verantwortlichen eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. MHS wird den Verantwortlichen bei der Umsetzung der Meldepflichten unterstützen. MHS wird dem Verantwortlichen insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Verantwortlichen verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung von MHS an den Verantwortlichen muss insbesondere folgende Informationen beinhalten:

a. 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;

b. eine Beschreibung der von MHS ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

5. Mitwirkungspflichten von MHS

a) MHS unterstützt den Verantwortlichen bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO.

b) MHS wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Verantwortlichen mit.

c) MHS unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

6. Kontrollbefugnisse

a) Der Verantwortliche hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen MHS und dem Verantwortlichen getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Verantwortlichen durch MHS im erforderlichen Umfang zu kontrollieren.

b) MHS ist dem Verantwortlichen gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Abs. a) erforderlich ist.

c) MHS und der Verantwortliche gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Art und Weise der Kontrolle unterliegen der individuellen Absprache zwischen MHS und des Verantwortlichen. Weitere Prüfungen sind unter Angabe des Anlasses zu begründen.

d) Nach Wahl von MHS kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Datenschutzbeauftragter) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Verantwortlichen in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 3** zu diesem Vertrag zu überzeugen.

e) MHS ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Verantwortlichen i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Verantwortliche ist darüber zu informieren.

7. Unterauftragsverhältnisse

a) MHS 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 Absatz b) genannten Voraussetzungen zulässig.

b) MHS hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen dem Verantwortlichen und MHS getroffenen Vereinbarungen einhalten kann. MHS 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. MHS wird den Verantwortlichen 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 Verantwortliche 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 Verantwortlichen jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann MHS das Vertragsverhältnis mit dem Verantwortlichen mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. MHS wird bei der Kündigungsfrist die Interessen des Verantwortlichen angemessen berücksichtigen. Wenn kein Widerspruch des Verantwortlichen binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Verantwortlichen zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers. Auf die Bedeutung seines Schweigens wird der Verantwortliche in der „Information“ gesondert hingewiesen.

c) MHS 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. Kann der Unterauftragnehmer keinen Datenschutzbeauftragten benennen so hat dieser verpflichtend den Datenschutzbeauftragten von MHS, oder der Datenschutzstelle, welche MHS nutzt, in Anspruch zu nehmen.

d) MHS hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Verantwortlichen auch gegenüber dem Unterauftragnehmer gelten.

e) MHS hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat MHS dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Verantwortlichem und MHS festgelegt sind. Dem Verantwortlichen ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln. Die elektronische Übermittlung ist dabei ausreichend.

f) MHS ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Verantwortlichen und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte des Verantwortlichen und der Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

g) Nicht als Unterauftragsverhältnisse i.S.d. Absätze a) bis f) sind Dienstleistungen anzusehen, die MHS 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 MHS für den Verantwortlichen erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. MHS 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.

8. Vertraulichkeitsverpflichtung

- a) MHS ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.
- b) MHS hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.
- c) Die Verpflichtung der Beschäftigten nach Abs. b sind dem Verantwortlichen auf Anfrage nachzuweisen.

9. Wahrung von Betroffenenrechten

- a) Der Verantwortliche ist für die Wahrung der Betroffenenrechte allein verantwortlich. MHS ist verpflichtet, den Verantwortlichen bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. MHS hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Verantwortlichen erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.
- b) Soweit eine Mitwirkung von MHS für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Verantwortlichen erforderlich ist, wird MHS die jeweils erforderlichen Maßnahmen nach Weisung des Verantwortlichen treffen. MHS wird den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.
- c) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Verantwortlichen bei MHS entstehen, bleiben unberührt.

10. Vergütung

Die Vergütung von MHS wird gesondert vereinbart.

11. Technische und organisatorische Maßnahmen zur Datensicherheit

a) MHS verpflichtet sich gegenüber dem Verantwortlichen zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

b) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. MHS und der Verantwortliche 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 MHS im Voraus mit dem Verantwortlichen abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, kann MHS ohne Abstimmung mit dem Verantwortlichen umsetzen. Der Verantwortliche kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der von MHS getroffenen technischen und organisatorischen Maßnahmen anfordern.

12. Dauer des Auftrags

a) Der Vertrag beginnt mit Zustimmung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über Nutzung der Dienstleistungen von MHS durch den Verantwortlichen.

b) Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von MHS gegen die anzuwendenden

Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, MHS eine Weisung des Verantwortlichen nicht ausführen kann oder will oder MHS den Zutritt des Verantwortlichen oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

13. Beendigung

Nach Beendigung des Vertrages hat MHS sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen 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

14. Schlussbestimmungen

- a) Diese Vereinbarung unterliegt deutschem Recht.
- b) Für Nebenabreden ist die Schriftform erforderlich.
- c) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht

Leipzig, den 15. April 2021

Ullrich Kastner

Geschäftsführer myhotelshop GmbH

Anlage 1

Leistungen von MHS - Umfang, Art und Zweck:

Erstellung von Platzierungen (Auswahl, Setup und Optimierung von Kampagnen), Consulting und Management (Entwicklung von Strategien im Onlinedirektvertrieb) und Webseitenservice (stärkere Conversions und gesteigerte Buchungserlebnisse).

Arten von Daten:

Jegliche durch MHS, innerhalb des Vertragsverhältnisses gespeicherte Daten, insbesondere von seinen Geschäftskunden, deren Mitarbeitern, nämlich Name, Anschrift, E-Mail-Adresse, ggf. Rufnummer sowie Details zur Kontaktnutzung und Auftragserfüllung.

Betroffene:

Mitarbeiter der Vertragspartner, sowie Kunden der Hotels.

Nutzung von Unterstützungsplattformen, durch MHS oder aus dem Unterauftragsverhältnis erkennbare Dritte, für die Erbringung der vertraglich festgesetzten Dienstleistungen:

Die Unterstützungsplattformen stellen ihrerseits eigene Unternehmen dar, welche ab dem 25.05. DSGVO-Konform arbeiten und handeln. MHS hat sich dieser Tatsache, ab Zeitpunkt der Zusammenarbeit zwischen MHS und Unterstützungsplattform/Unternehmen zu versichern. Diese Unternehmen können vom Verantwortlichen gesondert kontaktiert werden. Der Verantwortliche ist ebenfalls berechtigt, über MHS, nach Benennung eines berechtigten und begründeten Grundes, Auskunft über personenbezogene Daten des Verantwortlichen zu verlangen.

- easybill, easybill GmbH, Düsselstr. 21, 41564 Kaarst, Germany, <https://www.easybill.de/privacy>
- Google Ads, Google Tag Manager, Google Analytics sowie dazugehörige Anwendungen, Google Germany GmbH, ABC-Strasse 19, 20354 Hamburg, Germany, <https://policies.google.com/privacy>

- Microsoft Advertising, Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München, Germany, <https://privacy.microsoft.com/de-de/privacystatement>
- Matomo, ePrivacy Holding GmbH, Große Bleichen 21, 20354 Hamburg, Germany, <https://matomo.org/privacy-policy/>
- Mailchimp, The Rocket Science Group LLC d/b/a Mailchimp, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA, <https://mailchimp.com/legal/privacy/>
- Pipedrive, Pipedrive OÜ, Mustamäe tee 3a, Tallinn 10615, Estonia, <https://www.pipedrive.com/en/privacy>

Innerhalb der oben genannten Unterstützungsplattformen können Trackingverfahren angewendet werden, welche die Erbringung der Dienstleistung misst und somit zur Abrechenbarkeit selbiger führt. Tracking Devices:

- Cookies, welche folgende Datensätze anlegen: Ort / User Agent (Informationen über den Browser selbst) / Uhrzeit & Dauer des Zugriffs

Einsatz von Tools:

- Gutscheintools
- Chattools
- Newsletter-Subscription-Formulare
- Kontaktformulare
- Web-Font-Libraries

Anlage 2

MHS setzt derzeit folgende Unterauftragnehmer ein:

- Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4-6, 32339 Espelkamp, Germany, <https://www.mittwald.de/datenschutz>
- Websitebutler GmbH, Klosterstraße 62, 10179 Berlin, Germany, <https://www.websitebutler.de/de/datenschutz>
- DigitalOcean, LLC, 101 Avenue of the Americas, 10th Floor, New York, NY 10013 USA (Servers in Frankfurt a.M. (Germany) and Amsterdam (Netherlands)), <https://www.digitalocean.com/trust/>

Anlage 3

Technische und organisatorische Maßnahmen von MHS

MHS trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.:

1. Vertraulichkeit

a) Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Speicherung der Daten in einem Rechenzentrum / auf einem nicht allgemein zugänglichen Server, dort:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- dokumentierte Schlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung von Gästen in der Firma

- personelle Besetzung der Rechenzentren zu den Geschäftszeiten und ständige Erreichbarkeit der Personen, welche dafür verantwortlich sind

b) Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Umsetzung durch Benutzerkontensteuerung, Zugriff auf EDV-Systeme nur mit Benutzername/Passwort möglich.
- MHS vergibt selbst Passwörter, die nach erstmaliger Inbetriebnahme erneut geändert werden können.

c) Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Datenzugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Einrichtung eines Berechtigungskonzepts, bei dem einzelnen Kunden ausschließlich der Zugriff auf eigene Bereiche und Daten zugewiesen wird;
- Protokollierung des Zugriffs in Logfiles von MHS oder Dritten;
- Für die Geheimhaltung der Zugangsdaten und ggf. deren Weitergabe an Mitarbeiter ist der Verantwortliche selbst verantwortlich.

d) Zutritt-, Zugangs- und Zugriffskontrolle für und aus einem Drittland

Sollte es nach Einschätzung von MHS erforderlich werden, werden folgende Maßnahmen zur Sicherung des Zutritts, Zugangs und Zugriffs geprüft und angewendet:

- Verschlüsselung
- Pseudonymisierung
- Read-Only-Zugriff aus dem Drittland

e) Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Daten des Verantwortlichen werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
- Datensicherung erfolgt ebenfalls physikalisch oder logisch.

2. Integrität

a) Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Die Daten werden von MHS selbst eingegeben und verarbeitet,
- der Zugriff für MHS wird protokolliert, dies gilt insbesondere für den Zugriff auf Datenbanken oder Systeme des Verantwortlichen, in welchen personenbezogene Daten gespeichert sind.

b) Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Mitarbeiter sind auf das Datengeheimnis nach DSGVO und/oder § 53 BDSG (neu) verpflichtet,
- die Übertragung der Daten von und zu den Kundenbereichen erfolgt nur SSL-verschlüsselt,
- für die Einrichtung von Übertragungswegen auf externe Systeme (Datenexport) ist der Verantwortliche selbst verantwortlich.

3. Verfügbarkeit und Belastbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Daten des Verantwortlichen werden regelmäßigen Datensicherungen unterzogen,
- Einsatz redundanter Systeme,- Einsatz unterbrechungsfreier Stromversorgung.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Mitarbeiter von MHS werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Jeder Mitarbeiter wird spätestens am ersten Tag zu Beginn seiner Tätigkeit schriftlich zur Einhaltung der datenschutzrechtlichen

Anforderungen nach der DSGVO verpflichtet. Ohne Vorliegen dieser Erklärung erhält der Mitarbeiter keinen Zugriff auf personenbezogene Daten.