

## **Vereinbarung über Auftragsverarbeitung**

zwischen  
Sophy GmbH  
Lehmweg 17, 20251 Hamburg

- **Auftragnehmerin** -

und

- **Auftraggeberin** -

Die Auftraggeberin hat mit der Auftragnehmerin einen Hauptvertrag abgeschlossen. Die Auftragnehmerin wird im Rahmen der Leistungserbringung des Hauptvertrags personenbezogene Daten durch ihr Softwareprodukt für die Auftraggeberin, die als Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften gilt, verarbeiten.

### **1. Allgemeines**

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten im Auftrag und nach Weisung für die Auftraggeberin (im nachfolgenden: „Auftraggeber-Daten“). In dieser Vereinbarung als Datenverarbeitung“, „verarbeiten“ oder „Verarbeitung“ (von Auftraggeber-Daten) bezeichnete Vorgänge, beziehen sich allgemein auf die Verwendung von personenbezogenen Daten. Eine „Verwendung“ von Auftraggeber-Daten umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung, Anonymisierung, Pseudonymisierung, Verschlüsselung von Auftraggeber-Daten.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (Name, Vorname)
- Kommunikationsdaten (Anschrift, E-Mail-Adresse, Telefon)
- Freie Datenfelder (Auftraggeber definiert Datenart)

### **2. Gegenstand des Auftrags, Ort der Datenverarbeitung**

(1) Der Auftrag umfasst die im Hauptvertrag näher beschriebenen Leistungen. Der Kreis, der von der Datenverarbeitung betroffenen Personen umfasst

- Mitarbeiter des Auftraggebers
- Bewerber des Auftraggebers

(2) Die Verarbeitung der Auftraggeber-Daten durch die Auftragnehmerin findet ausschließlich in Mitgliedstaaten der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Eine Datenverwendung außerhalb des genannten Gebiets, auch im Wege der Gewährung des Zugriffs auf Auftraggeber-Daten an Personen außerhalb des genannten Gebiets, bedarf der vorherigen schriftlichen Zustimmung der Auftraggeberin. Datenverwendungen in Ländern, die weder Mitgliedstaat der Europäischen Union noch Vertragsstaat des EWR sind („Drittstaaten“) dürfen nur unter der weiteren Voraussetzung erfolgen, dass die Voraussetzungen der Art. 44 ff. DS-GVO hinreichend erfüllt sind.

(3) Die Auftragnehmerin erwirbt an den Auftraggeber-Daten keinerlei Rechte.

### **3. Rechte und Pflichten der Auftraggeberin**

- (1) Die Auftraggeberin ist Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO für die Verarbeitung von Auftraggeber-Daten im Auftrag durch die Auftragnehmerin.
- (2) Die Auftraggeberin steht gegenüber Dritten und den Betroffenen für die Wahrung der Betroffenenrechte nach Art. 15 ff. DS-GVO ein. Betroffenenrechte sind gegenüber der Auftraggeberin geltend zu machen.
- (3) Die Auftraggeberin gilt als Eigentümerin der Auftraggeber-Daten und im Verhältnis der Parteien zueinander Inhaber aller etwaigen Rechte an den Auftraggeber-Daten.
- (4) Für die Erfüllung von Informationspflichten gegenüber Dritten nach Art. 34 DS-GVO ist die Auftraggeberin verantwortlich.

#### **4. Pflichten der Auftragnehmerin, Datensicherheit**

- (1) Die Auftragnehmerin verarbeitet Auftraggeber-Daten ausschließlich im Rahmen der getroffenen Vereinbarungen, den gesetzlichen Pflichten und entsprechend den Weisungen der Auftraggeberin.
- (2) Die Auftragnehmerin darf ohne vorherige Zustimmung in Textform durch die Auftraggeberin keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen, soweit und solange sie nicht zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Die Auftragnehmerin darf Auftraggeber-Daten ohne vorherige schriftliche Zustimmung durch die Auftraggeberin auch nicht an Dritte oder andere Empfänger aushändigen. Hiervon ausgenommen sind Datenweitergaben an Unterauftragnehmer, deren Beauftragung die Auftraggeberin gemäß Ziffer 6.1 zugestimmt hat.
- (3) Die Auftragnehmerin wird die Daten, die sie im Auftrag für die Auftraggeberin verarbeitet, auf geeignete Weise kennzeichnen und von sonstigen Datenbeständen getrennt halten.
- (4) Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird die Auftragnehmerin die Daten mit dem jeweiligen Zweck kennzeichnen.
- (5) Die Auftragnehmerin stellt der Auftraggeberin auf Verlangen unverzüglich ein jeweils aktuelles Verzeichnis nach Art. 30 Abs. 2 und 3 DS-GVO zur Verfügung.
- (6) Die Auftragnehmerin ist nicht verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Im Falle der Bestellung eines Datenschutzbeauftragten teilt die Auftragnehmerin dessen Kontaktdaten mit.
- (7) Die Auftragnehmerin ist verpflichtet, ihr Unternehmen und ihre Betriebsabläufe so zu gestalten, dass die Auftraggeber-Daten im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Die Auftragnehmerin wird die Auftraggeberin über Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, rechtzeitig vorab informieren.
- (8) Die Auftragnehmerin ist verpflichtet, der Auftraggeberin jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen der Auftraggeberin unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch sie oder andere mit der Verarbeitung beschäftigten Personen oder von ihr eingesetzte Unterauftragnehmer erfolgt ist.
- (9) Für den Fall, dass die Auftragnehmerin feststellt oder Tatsachen die Annahme begründen, dass von ihr für die Auftraggeberin verarbeitete

- besondere Arten personenbezogener Daten (Art. 9 DS-GVO) oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten (Art. 10 DS-GVO) beziehen

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind oder Datenverarbeitungsvorgänge erfolgen, die einer Datenschutzfolgenabschätzung bedürfen, hat die Auftragnehmerin die Auftraggeberin unverzüglich und vollständig über Zeitpunkt, Art und Umfang in Schrift- oder Textform (Fax/E-Mail) zu informieren. Die Auftragnehmerin ist überdies verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch die Auftragnehmerin getroffen wurden, um dies künftig zu verhindern.

(10) Die Auftragnehmerin ist verpflichtet, der Auftraggeberin eine Verletzung des Schutzes personenbezogener Daten unverzüglich zu melden und sie bei ihren diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen auf erstes Anfordern im Rahmen des Zumutbaren zu unterstützen. Die Auftragnehmerin wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeber-Daten zu minimieren und zu beseitigen, die Auftraggeber-Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.

## **5. Umfang der Weisungsbefugnis**

(1) Die Auftraggeberin hat das Recht, ergänzende Weisungen über Art und Umfang der Datenverarbeitung zu erteilen.

(2) Die Auftragnehmerin wird die Auftraggeberin unverzüglich darüber informieren, wenn eine von der Auftraggeberin erteilte Weisung nach ihrer Auffassung gegen gesetzliche Regelungen verstößt.

## **6. Unterauftragsverhältnisse**

(1) Die Beauftragung von Unterauftragnehmern durch die Auftragnehmerin ist nur mit vorheriger schriftlicher Zustimmung zulässig. Der Beauftragung der in **Anlage 1** genannten Unterauftragnehmer hat die Auftraggeberin zugestimmt.

(2) Die Auftragnehmerin hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen den Parteien getroffenen Vereinbarungen einhalten kann.

(3) Die Auftragnehmerin hat den Unterauftragnehmer in dem Unterauftragsverarbeitungsvertrag schriftlich ebenso zu verpflichten, wie auch die Auftraggeberin aufgrund dieses Vertrags gegenüber der Auftraggeberin verpflichtet ist. In dem Unterauftragsverarbeitungsvertrag sind die Verantwortlichkeitssphären der Auftragnehmerin und des Unterauftragnehmers klar voneinander abzugrenzen. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen den einzelnen Unterauftragnehmern. Die Auftragnehmerin haftet für ein Verschulden ihrer Unterauftragnehmer wie für eigenes Verschulden.

(4) Eine Übergabe von Daten an den Unterauftragnehmer ist erst zulässig, wenn alle Voraussetzungen für eine Unterbeauftragung vorliegen und der Unterauftragnehmer die Verpflichtung nach Ziffer 8 dieses Vertrags erfüllt hat.

(5) Die Auftragnehmerin hat abgeleitete Kontrollpflichten gegenüber ihren Unterauftragnehmern, die im Rahmen dieses Vertrags wahrzunehmen sind. Die Auftragnehmerin hat die Einhaltung der vertraglichen Verpflichtungen des Unterauftragnehmers regelmäßig in geeigneter Form zu überprüfen, das Ergebnis der Prüfung zu dokumentieren und den entsprechenden Prüfbericht der Auftraggeberin auf Anfrage zur Verfügung zu stellen. Die Auftraggeberin bleibt berechtigt, die Ausübung der Kontrollbefugnisse durch die Auftragnehmerin uneingeschränkt zu überwachen.

## **7. Kontrollbefugnisse**

(1) Die Auftraggeberin hat das Recht, die Verarbeitung von Auftraggeber-Daten durch die Auftragnehmerin im erforderlichen Umfang zu kontrollieren. Die Auftragnehmerin stellt insbesondere sicher, dass sich die Auftraggeberin von der Einhaltung der Pflichten der Auftragnehmerin nach Art. 28 DS-GVO überzeugen kann.

(2) Die Auftragnehmerin ist der Auftraggeberin gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Die Auftraggeberin kann eine Einsichtnahme in die von der Auftragnehmerin für die Auftraggeberin verarbeiteten Auftraggeber-Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Die Auftraggeberin kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte der Auftragnehmerin zu den jeweils üblichen Geschäftszeiten vornehmen. Wenn Unterauftragsverhältnisse bestehen, dann wird die Auftragnehmerin im Auftrag und nach Weisungen der Auftraggeberin diese Kontrollen der jeweiligen Betriebsstätte(n)

durchführen. Die Auftraggeberin wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe der Auftragnehmerin durch die Kontrollen gestört werden.

(5) Gemäß den anwendbaren Datenschutzvorschriften unterliegen die Auftraggeberin und die Auftragnehmerin öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen der Auftraggeberin wird die Auftragnehmerin die Auftraggeberin im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist. Die Auftragnehmerin wird insbesondere auf Verlangen der Auftraggeberin ihr selbst oder der Aufsichtsbehörde unmittelbar alle Informationen im Zusammenhang mit diesem Vertrag geben und entsprechende Auskünfte erteilen und der Aufsichtsbehörde die Möglichkeit einräumen, Prüfungen in demselben Umfang durchzuführen wie sie die Aufsichtsbehörde bei der Auftraggeberin durchführen darf. Die Auftragnehmerin gewährt der zuständigen Aufsichtsbehörde auch in diesem Rahmen alle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. Falls die Aufsichtsbehörde bei der Auftragnehmerin Kontrollhandlungen, Ermittlungen oder Maßnahmen durchführt, die Auftraggeber-Daten betreffen, hat die Auftragnehmerin die Auftraggeberin darüber so früh wie möglich und in der Regel unverzüglich nach Erhalt der Ankündigung der Aufsichtsmaßnahme durch die Behörde zu informieren.

## **8. Vertraulichkeit**

(1) Die Auftragnehmerin ist bei der Verarbeitung von Auftraggeber-Daten zur Wahrung der Vertraulichkeit verpflichtet. Die Auftragnehmerin verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie der Auftraggeberin obliegen. Die Auftraggeberin ist verpflichtet, der Auftragnehmerin etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Die Auftragnehmerin sichert zu, dass ihr die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und sie mit deren Anwendung vertraut ist. Die Auftragnehmerin sichert ferner zu, dass sie die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO wahrt und bei der Durchführung der Arbeiten nur Beschäftigte bzw. freie Mitarbeiter einsetzt, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Auftragnehmerin und jede der Auftragnehmerin unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung der Auftraggeberin verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Auftragnehmerin wird diese Verpflichtungen schriftlich dokumentieren. Auf Verlangen der Auftraggeberin wird die Auftragnehmerin ihr die Einhaltung dieser Bestimmung durch Vorlage der Verpflichtungserklärungen oder auf andere geeignete Weise nachweisen.

## **9. Wahrung von Betroffenenrechten**

(1) Die Auftraggeberin ist für die Wahrung der Betroffenenrechte allein verantwortlich. Soweit ein Betroffener sich unmittelbar an die Auftragnehmerin zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Auftraggeber-Daten wenden sollte, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten und ohne entsprechende dokumentierte Einzelweisung der Auftraggeberin nicht mit dem Betroffenen in Kontakt treten. Die Auftragnehmerin darf Auskünfte an Betroffene nur nach vorheriger Weisung durch die Auftraggeberin erteilen.

(2) Soweit eine Mitwirkung der Auftragnehmerin für die Wahrung von Betroffenenrechten – insbesondere solche auf Auskunft, Berichtigung, Sperrung, Löschung, Datenportabilität – durch die Auftraggeberin erforderlich ist, wird die Auftragnehmerin die jeweils erforderlichen Maßnahmen nach Weisung der Auftraggeberin treffen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen der Auftraggeberin bei der Auftragnehmerin entstehen, bleiben unberührt.

## **10. Geheimhaltungspflichten**

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

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

### **11. Technische und organisatorische Maßnahmen zur Datensicherheit (Anlage 2)**

Die Auftragnehmerin verpflichtet sich gegenüber der Auftraggeberin, die Sicherheit gem. Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO durch technische und organisatorische Maßnahmen sicherzustellen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragnehmerin gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

### **12. Dauer des Auftrags, Beendigung**

(1) Der Vertrag beginnt mit Unterzeichnung durch den Auftraggeber und endet mit Beendigung des Hauptvertrags.

(2) Die Auftraggeberin kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der Auftragnehmerin gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, die Auftragnehmerin eine Weisung der Auftraggeberin nicht ausführen kann oder will oder die Auftragnehmerin den Zutritt der Auftraggeberin oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

### **13. Rückgabe und Löschung überlassener Daten**

(1) Der Auftragnehmerin ist es untersagt, nach Beendigung dieses Vertrags Auftraggeber-Daten aktiv zu verarbeiten; nur eine weitere Speicherung der Auftraggeber-Daten bleibt zugelassen, bis die Auftragnehmerin diese Auftraggeber-Daten bestimmungsgemäß an die Auftraggeberin herausgegeben oder sie gelöscht oder vernichtet hat; in diesem Fall gelten die Bestimmungen dieses Vertrags auch nach Beendigung des Vertrags bis zu dem Zeitpunkt weiter, in dem die Auftragnehmerin über keinerlei Auftraggeber-Daten mehr verfügt.

(2) Die Auftragnehmerin hat sämtliche ihr von der Auftraggeberin überlassenen sowie sämtliche im Zuge der Vertragsdurchführung hinzugewonnenen Auftraggeber-Daten und alle Verarbeitungs- und Nutzungsergebnisse hieraus vollständig und unwiederbringlich an die Auftraggeberin herauszugeben bzw. zu löschen bzw. zu vernichten, sobald ihre Kenntnis für die Erfüllung des Zwecks der jeweiligen Erhebung und Verwendung nicht mehr erforderlich ist, spätestens jedoch nach Beendigung der vertragsgegenständlichen Leistungserbringung. Den Parteien ist bekannt, dass es technisch nicht immer möglich ist, gezielt Daten der Auftraggeberin zu löschen. In diesen Fällen verpflichtet sich die Auftragnehmerin, die Daten – soweit möglich – zu deaktivieren bzw. nicht mehr aktiv zu nutzen oder nutzbar zu erhalten.

(3) Die Auftragnehmerin dokumentiert die Maßnahmen nach Ziffer 13.2 in geeigneter Weise und bestätigt der Auftraggeberin die vollständige und vertragsgemäße Rückgabe bzw. Vernichtung/Löschung der Datenträger und Daten. Die Auftraggeberin ist befugt, dies zu kontrollieren. Ziffer 7 gilt entsprechend.

(5) Die Auftragnehmerin hat hinsichtlich der Datenträger und Auftraggeber-Daten kein Zurückbehaltungsrecht.

### **14. Haftung**

Auftraggeberin und Auftragnehmerin haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Im Innenverhältnis gilt Art. 28 Abs. 4 S. 2 DS-GVO. Unbeschadet der Artikel 82, 83 und 84 DS-GVO gilt die Auftragnehmerin, wenn sie unter Verstoß gegen datenschutzrechtliche Regelungen die Zwecke und Mittel der Verarbeitung bestimmt und insbesondere die Weisungen der Auftraggeberin überschreitet, in Bezug auf diese Verarbeitung als Verantwortliche.

#### **15. Schlussbestimmungen**

(1) Änderungen, Ergänzungen und die Aufhebung dieses Vertrags bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DS-GVO am besten gerecht wird.

Hamburg, den

# Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen nach Artikel 32 Absatz 1 DSGVO

**Verantwortlicher/Auftragsverarbeiter:**

SOPHY GmbH, Lehmweg 17, 20251 Hamburg

Geschäftsführer: Oliver Knoblauch

Amtsgericht Hamburg HRB 154658

<b>Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen</b>	
1 Pseudonymisierung	<ul style="list-style-type: none"> <li>▪ Die IT-Systeme werden durch entsprechende datenschutzfreundliche Voreinstellungen auf das zur Erfüllung des Vertragszwecks erforderliche Maß beschränkt und dementsprechend nur diejenigen personenbezogenen Daten verarbeitet, die für den verfolgten Zweck auch erforderlich sind. Zielvorgabe ist Datensparsamkeit durch Trennung von personenbezogenen Identifizierungsmerkmalen und Inhaltsdaten, die Verwendung von Pseudonymen und Anonymisierung sowie die Löschung personenbezogener Daten, sobald diese zur Erreichung des verfolgten Zwecks nicht mehr benötigt werden.</li> </ul>
2 Verschlüsselung	<ul style="list-style-type: none"> <li>▪ mobile Arbeitsplatzrechner werden mindestens durch Verschlüsselung der Home-Laufwerke, durch eingebaute Mechanismen (wie z.B. FileVault oder Bitlocker) geschützt</li> <li>▪ Daten, die einen hohen Schutzbedarf aufweisen werden nicht auf vernetzten Arbeitsplatzrechnern gehalten</li> <li>▪ Vertrauliche Daten sollen unter Berücksichtigung geeigneter Maßnahmen entsprechend der Kategorisierung der Daten versendet werden (Verschlüsselung).</li> </ul>
3 Vertraulichkeit	Die Daten werden nach ISO 27001, SOC 2/3 und PCI DSS 3.0 im Google Rechenzentrum Frankfurt gespeichert
4 Integrität	<p>Zur Verhinderung der unberechtigten Änderung von personenbezogenen Daten dienen unter anderem:</p> <ul style="list-style-type: none"> <li>▪ Berechtigungs- und Zugriffskonzepte               <ul style="list-style-type: none"> <li>Berechtigungsmechanismus mit Möglichkeit zur exakten Differenzierung</li> <li>Revisionssicheres, verbindliches Berechtigungsvergabeverfahren</li> </ul> </li> <li>▪ Trennungskontrolle</li> </ul>

<b>Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen</b>	
	<p>Die personenbezogenen Daten des Auftraggebers liegen logisch voneinander getrennt und exakt zuordenbar auf unseren technischen Einrichtungen.</p> <ul style="list-style-type: none"> <li>▪ Eingabekontrolle Alle administrativen Tätigkeiten (z.B. Einrichtung und Änderung von Backups, Software-Updates u.a.), die der Auftragnehmer aufgrund organisatorischer Vereinbarungen für den Auftraggeber ausführt, werden grundsätzlich protokolliert und sind über den vorgeschriebenen Zeitraum nachvollziehbar.</li> </ul>
5 Verfügbarkeit	<ul style="list-style-type: none"> <li>▪ Verfügbarkeitskontrolle wird sichergestellt durch das Google Rechenzentrum</li> <li>▪ Auftragskontrolle</li> </ul> <p>Die personenbezogenen Daten des Auftraggebers werden ausschließlich auf der Grundlage der vertraglich festgelegten Regelungen und zusätzlicher schriftlicher Weisungen verarbeitet.</p>
6 Belastbarkeit	<p>Die Systeme und Dienste müssen so ausgelegt sein, dass sie auch bei punktuell hohen oder dauerhaft hohen Belastungen von Verarbeitungen leistungsfähig bleiben</p> <p>Hierzu zählen unter anderem:</p> <ul style="list-style-type: none"> <li>▪ Speicherkapazitäten</li> <li>▪ Zugriffskapazitäten</li> <li>▪ Leitungskapazitäten</li> </ul>
7 Physischer oder technischer Zwischenfall	<p>Zur schnellen Wiederherstellung von Systemen und Datenbanken bei physischen oder technischen Zwischenfällen dienen unter anderem:</p> <ul style="list-style-type: none"> <li>▪ Backup-Konzepte</li> <li>▪ Redundante Datenspeicherung</li> <li>▪ Cloud-Services</li> </ul>
8 Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM	<p>Hierzu zählen unter anderem:</p> <ul style="list-style-type: none"> <li>▪ Regelmäßige Prüfung IT-Infrastruktur</li> <li>▪ Regelmäßige Prüfung durch unabhängigen Datenschützer</li> </ul>

Hamburg, 16.08.2019

  
 Verantwortlicher/Auftragnehmer