DATENSCHUTZNACHTRAG

Dieser Datenschutznachtrag (**„Nachtrag“**) ist Bestandteil des Dienstleistungsvertrages zwischen (**„Planet“**) und (**„Händler“**) vom (**„Vertrag“**).

Planet und der Händler (jeweils einzeln als **„Partei“** und gemeinsam als **„Parteien“** bezeichnet) vereinbaren, dass dieser Nachtrag die für die Verarbeitung personenbezogener Daten (bzw. gemeinsam genutzter personenbezogener Daten) durch die Parteien für die im Vertrag und/oder diesem Nachtrag genannten Zwecke geltenden Datenschutzanforderungen regelt.

1. Begriffsbestimmungen

In diesem Nachtrag gelten die folgenden Definitionen:

1.1. **Verbundene Unternehmen:** alle natürlichen oder juristischen Personen, Partnerschaften, Verbände oder Unternehmen, die direkt oder indirekt über eine oder mehrere Zwischenstellen, die je nach Sachlage eine Partei kontrolliert, von ihr kontrolliert wird oder mit ihr unter gemeinsamer Kontrolle steht, sowie deren jeweiligen Nachfolger. Der Begriff „Kontrolle“ einschließlich der Begriffe „kontrolliert“, „kontrolliert von“ und „unter gemeinsamer Kontrolle stehend mit“ bezeichnet den direkten oder indirekten Besitz der Möglichkeit, die Ausrichtung des Managements und der Politik eines Unternehmens, einer Partnerschaft, eines Verbandes oder eines Unternehmens durch den Besitz stimmberechtigter Aktien, durch Vertrag oder auf sonstige Weise zu bestimmen oder dies zu veranlassen. Verbundene Unternehmen sind weiterhin auch alle derzeit bestehenden oder später durch Investitionen, Fusionen oder auf andere Weise gegründete Unternehmen einschließlich der Rechtsnachfolger und Bevollmächtigten dieser Unternehmen.

1.2. **Geltende Gesetze:** alle in der jeweiligen Rechtsordnung einschlägigen Gesetze, Verordnungen, Regierungsbeschlüsse, Bestimmungen, Leitlinien und deren Änderungen sowie alle von relevanten und zuständigen Regierungsstellen in allen für den Vertrag relevanten Rechtsordnungen gefassten Beschlüsse einschließlich unter anderem Vorschriften für die Tätigkeit einer zwischengeschalteten Bank und aller in den jeweiligen Ländern geltenden Währungs- und Finanzvorschriften, Rechtsvorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, sowie zu Embargos, Sanktionen, Bestechung, Fehlverhalten, vertraulichen Informationen (einschließlich geistigen Eigentums und Geschäftsgeheimnissen), Verhalten von Finanzinstituten und Datenschutzgesetzen.

1.3. **Verantwortlicher:** hat die für den Begriff „Verantwortlicher“ geregelte Bedeutung, wenn dieser die Zwecke der personenbezogenen Daten und die Mittel zu deren Verarbeitung gemäß den Datenschutzgesetzen bestimmt.

1.4. **Auftragsverarbeiter:** hat die für den Begriff „Auftragsverarbeiter“ geregelte Bedeutung, wenn eine andere Stelle personenbezogene Daten im Auftrag eines Verantwortlichen gemäß den Datenschutzgesetzen verarbeitet.

1.5. **Datenschutzgesetze:** die Datenschutz-Grundverordnung 2016/679 (DSGVO), das neue Schweizer Bundesgesetz über den Datenschutz (nFADP), der UK Data Protection Act 2018, die UK Privacy and Electronic Communications Regulations 2003, das französische Gesetz n° 78-17 vom 6. Januar 1978 über Informationstechnologie, Dateien und Freiheiten sowie alle anderen einschlägigen, sich auf die Verarbeitung personenbezogener Daten beziehenden Gesetze jeweils in ihrer aktuell gültigen Fassung.

1.6. **Datensicherheitszwischenfall:** bezeichnet Zugriff, Verarbeitung, Löschung sowie Verlust auf unbefugte oder versehentliche Weise oder jede Form der unrechtmäßigen Verarbeitung der personenbezogenen Daten (bzw. der gemeinsam genutzten personenbezogener Daten) und/oder zu Zerstörung, Verlust, Änderung, unbefugte Weitergabe oder Zugriff auf die personenbezogenen Daten (bzw. die gemeinsam genutzten personenbezogenen Daten) auf versehentliche oder unrechtmäßige Weise führende Verletzung der Sicherheit und/oder Vertraulichkeit.

1.7. **Betroffene Person:** eine identifizierte oder identifizierbare natürliche Person, auf die sich personenbezogene Daten beziehen.

1.8. **Antrag einer betroffenen Person:** bezeichnet einen von einer betroffenen Person gestellten förmlichen Antrag mit dem Ziel, ihre Rechte auszuüben, und zwar (i) auf Zugriff auf ihre personenbezogenen Daten, (ii) auf Berichtigung oder Löschung ihrer personenbezogenen Daten, (iii) auf Einschränkung der Verarbeitung ihrer personenbezogenen Daten oder auf einen Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten, (iv) auf Antrag auf

Übertragbarkeit ihrer personenbezogenen Daten, (v) darauf, nicht Gegenstand einer automatisierten Entscheidungsfindung (einschließlich Profiling) zu sein, oder (vi) in Bezug auf jedes andere der betroffenen Person in jeder einschlägigen Rechtsordnung, für die dieser Nachtrag gilt, zustehende Recht.

1.9. **Personenbezogene Daten:** alle eine einzelne Person identifizierenden (wie in den Datenschutzgesetzen geregelt) und im Zusammenhang mit dem Vertrag verarbeiteten personenbezogenen Daten.

1.10. **Gemeinsam genutzte personenbezogene Daten:** alle eine einzelne Person identifizierenden (wie in den Datenschutzgesetzen geregelt) und im Zusammenhang mit dem Vertrag verarbeiteten personenbezogenen Daten, wenn die Parteien als unabhängige Verantwortliche im Rahmen einer „Beziehung von Verantwortlichem zu Verantwortlichem“ handeln.

1.11. **Standardvertragsklauseln:** sind (i) die von der Europäischen Kommission am 4. Juni 2021 veröffentlichten und von ihr angenommenen Standardvertragsklauseln für die Übermittlung personenbezogener Daten aus dem EWR in Drittländer (abrufbar auf der Website der Europäischen Kommission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en) und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (**„Schweizerischer EDÖB“**) für Datenübermittlungen in Drittländer (zusammen „**EU-Standardvertragsklauseln“**), (ii) das vom UK Information Commissioner’s Office („**UK ICO**“) für Datenübermittlungen aus dem Vereinigten Königreich in Drittländer angenommene internationale Datenübermittlungs-Addendum (**„UK Transfer Addendum“**), (iii) alle von einer Datenschutzaufsichtsbehörde in Bezug auf Datenübermittlungen in Drittländer angenommenen derartigen vergleichbaren Klauseln (soweit anwendbar) oder (iv) alle Nachfolgeklauseln zu (i) bis (iii).

1.12. **Unterauftragsverarbeiter:** bezeichnet eine vom Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten im Namen des Auftragsverarbeiters beauftragte Stelle.

1.13. **Aufsichtsbehörde:** bezeichnet eine unabhängige öffentliche Behörde, die entweder: (i) von einem EU-Mitgliedstaat gemäß Artikel 51 der DSGVO eingerichtet wurde, oder (ii) die für Sie für den Datenschutz zuständige Behörde.

2. Datenschutzrollen

Im Zuge der Erbringung der von Planet dem Händler im Rahmen des Vertrages angebotenen Dienstleistungen können die Parteien von Zeit zu Zeit personenbezogene Daten an die andere Partei weitergeben oder dieser zur Verfügung stellen. Die Parteien vereinbaren, dass je nach den beauftragten Dienstleistungen die ihnen jeweils zugewiesenen Datenschutzrollen für die Zwecke der Datenschutzgesetze entweder (i) unabhängige für die Datenverarbeitung Verantwortliche (im Rahmen einer Beziehung von Verantwortlichem zu Verantwortlichem), (ii) Verantwortlicher (im Rahmen einer Beziehung von Auftragsverarbeiter zu Verantwortlichem) oder (iii) Auftragsverarbeiter im Auftrag der anderen Partei (im Rahmen einer Beziehung von Auftragsverarbeiter zu Verantwortlichem) sind. Dies vorausgeschickt:

a) **Wenn die Parteien personenbezogene Daten als unabhängige Verantwortliche verarbeiten, gilt § 3 dieses Nachtrags.**
b) **Wenn eine als Verantwortlicher im Rahmen einer Beziehung von Verantwortlichem zu Auftragsverarbeiter handelnde Partei personenbezogene Daten verarbeitet, gilt § 4 dieses Nachtrags für diese Partei.**
c) **Wenn eine als Auftragsverarbeiter im Auftrag der anderen Partei handelnde Partei personenbezogene Daten verarbeitet, gilt § 5 dieses Nachtrags für diese Partei.**

Anlage 1 enthält eine vollständige Beschreibung der Rollen und Zwecke, für die personenbezogene Daten (bzw. gemeinsam genutzte personenbezogene Daten) im Zusammenhang mit den vertragsgegenständlichen Dienstleistungen verarbeitet werden.

3. Pflichten der als unabhängige Verantwortliche handelnde Parteien

Dieser § 3 gilt für den Fall, dass die Parteien als unabhängige Verantwortliche handeln.

3.1. Allgemeines

3.1.1. Die Parteien legen einander regelmäßig personenbezogene Daten für die im Vertrag und/oder im Nachtrag geregelten Zwecke offen (**„gemeinsam genutzte personenbezogene Daten“**) und vereinbaren, dass jede Partei in Bezug auf diese gemeinsam genutzten personenbezogenen Daten unabhängig und für sich selbst als Verantwortlicher handelt und die Zwecke und Mittel der betreffenden Datenverarbeitung unabhängig bestimmt.

3.2. Verarbeitung gemeinsam genutzter personenbezogener Daten

3.2.1. Soweit eine Partei als für die gemeinsam genutzten personenbezogenen Daten Verantwortlicher in Bezug auf Dienstleistungen handelt, ist diese für die Einhaltung und Erfüllung ihrer Pflichten gemäß den Datenschutzgesetzen verantwortlich und muss insbesondere

a) sicherstellen, dass die im Rahmen des Vertrages bereitgestellten oder zugänglich gemachten gemeinsam genutzten personenbezogenen Daten korrekt und aktuell sind,
b) sicherstellen, dass sie über eine angemessene Rechtsgrundlage für die Verarbeitung der gemeinsam genutzten personenbezogenen Daten verfügt, wie in diesem Nachtrag und/oder dem Vertrag geregelt,
c) sicherstellen, dass den von der Datenverarbeitung betroffenen Personen zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten alle erforderlichen Hinweise zur angemessenen Verarbeitung (allgemein als „Datenschutzhinweise“ oder „Datenschutzrichtlinien“ bezeichnet) zur Verfügung gestellt werden, um die rechtmäßige Verarbeitung (einschließlich der Erhebung und Weitergabe) der gemeinsam genutzten personenbezogenen Daten für die im Vertrag und/oder dem Nachtrag geregelten Zwecke zu ermöglichen,
d) sicherstellen, dass, sofern keine andere in den Datenschutzgesetzen enthaltene Rechtsgrundlage die Rechtmäßigkeit der Verarbeitung begründet, alle erforderlichen Einwilligungen der betroffenen Personen in die Verarbeitung eingeholt und aufgezeichnet werden, und im Fall des Widerrufs einer Einwilligung durch eine betroffene Person sicherstellen, dass dies der anderen Partei mitgeteilt wird.

3.2.2. Jede Partei verpflichtet sich, der anderen Partei keine nicht für die Erbringung der Dienstleistungen erforderlichen speziellen Kategorien personenbezogener Daten (beispielsweise Gesundheitsdaten) zu übermitteln.

3.3. Datensicherheit

3.3.1. Jede Partei gewährleistet durch angemessene Maßnahmen die Zuverlässigkeit der zur Verarbeitung gemeinsam genutzter personenbezogener Daten berechtigten Personen und stellt sicher, (i) dass der Zugriff streng auf die Personen beschränkt ist, die für die im Vertrag und/oder in diesem Nachtrag geregelten Zwecke Kenntnis von den betreffenden gemeinsam genutzten personenbezogenen Daten oder Zugriff auf diese haben müssen, und (ii) dass diese Personen Vertraulichkeitsverpflichtungen oder beruflichen oder gesetzlichen Geheimhaltungspflichten unterliegen.

3.3.2. Die Parteien ergreifen und unterhalten geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus (unter Berücksichtigung von Art, Umfang, Kontext und Zwecken der Verarbeitung) auch im Hinblick auf eine unbefugte oder unrechtmäßige Verarbeitung oder einen versehentlichen Verlust oder eine versehentliche Zerstörung oder Beschädigung solcher gemeinsam genutzter personenbezogener Daten. Insbesondere wird Planet die folgenden unter https://www.weareplanet.com/technical-and-organisational-measures abrufbaren und zusammengefasst in Anlage 2 dargestellten technischen und organisatorischen Maßnahmen anwenden.

3.3.3. Die die gemeinsam genutzten personenbezogenen Daten erhaltende Partei darf diese nicht länger als für die im Vertrag und/oder in diesem Nachtrag geregelten Zwecke erforderlich aufbewahren oder verarbeiten und ist für die Durchführung geeigneter Maßnahmen verantwortlich, um sicherzustellen, dass die gemeinsam genutzten personenbezogenen Daten vernichtet oder gelöscht werden, wenn sie für diese Zwecke nicht mehr erforderlich sind. Ungeachtet dessen kann jede Partei die gemeinsam genutzten personenbezogenen Daten nach Maßgabe der geltenden gesetzlichen oder berufsständischen Aufbewahrungsfristen weiter aufbewahren.

3.4. Rechte betroffener Personen

3.4.1. Jede Partei ist für die Bearbeitung ihrer eigenen Anträge betroffener Personen in Bezug auf die gemeinsam genutzten personenbezogenen Daten verantwortlich und leistet der anderen Partei die nach billigem Ermessen erforderliche Unterstützung, damit diese den Anträgen dieser betroffenen Personen nachkommen kann.

3.4.2. Wenn eine Partei einen Antrag einer betroffenen Person in Bezug auf die gemeinsam genutzten personenbezogenen Daten, der eine Verarbeitung betrifft, für die die andere Partei der Verantwortliche ist, erhält, leitet die diesen Antrag

der betroffenen Person erhaltende Partei diesen unverzüglich an die andere Partei weiter. Auf billiges schriftliches Verlangen hin leistet die den Antrag der betroffenen Person erhaltende Partei der anderen Partei angemessene Zusammenarbeit und Unterstützung, damit die andere Partei dem Antrag der betroffenen Person nachkommen und die in den Datenschutzgesetzen geregelten Fristen einhalten kann.

3.5. Datensicherheitszwischenfälle

3.5.1. Wenn eine Partei Kenntnis von einem sich wesentlich auf die Verarbeitung der gemeinsam genutzten personenbezogenen Daten auswirkenden Datensicherheitszwischenfall erhält, benachrichtigt sie unverzüglich die andere Partei und arbeitet mit dieser zusammen, damit die andere Partei eine Untersuchung des Zwischenfalls durchführen, eine angemessene Reaktion formulieren und geeignete weitere Schritte in Bezug auf den Datensicherheitszwischenfall unternehmen kann.

3.5.2. Wenn ein Datensicherheitszwischenfall in Bezug auf die gemeinsam genutzten personenbezogenen Daten eintritt oder der Verdacht besteht, dass ein Datensicherheitszwischenfall eingetreten ist oder eintreten könnte, informiert jede Partei die andere Partei so schnell wie möglich schriftlich mit allen relevanten Informationen über die Einzelheiten des Zwischenfalls, damit diese Partei die Datenschutzgesetze einhalten kann. Zu den relevanten Informationen über den Datensicherheitszwischenfall gehören:

a) Name, Handelsname und mutmaßlich betroffene Informationen,
b) Beschreibung der Art des Zwischenfalls einschließlich nach Möglichkeit der Kategorien und der ungefähren Zahl betroffener Personen,
c) Name und Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle, bei der weitere Informationen eingeholt werden können,
d) Beschreibung der voraussichtlichen Folgen,
e) Beschreibung der ergriffenen oder zu ergreifenden Maßnahmen für die Behandlung des Zwischenfalls, gegebenenfalls einschließlich Maßnahmen zur Abschwächung seiner möglichen nachteiligen Auswirkungen sowie
f) Kopie des gesamten Schriftverkehrs in diesem Zusammenhang einschließlich des Schriftverkehrs mit allen betroffenen Personen.

3.6. Gegenseitige Unterstützung

3.6.1. Jede Partei gewährt der anderen Partei auf billiges Ersuchen hin angemessene Unterstützung, Informationen und Zusammenarbeit, um die Einhaltung ihrer jeweiligen Pflichten gemäß den Datenschutzgesetzen zu gewährleisten.

3.6.2. Wenn eine Partei eine Beschwerde, einen Bescheid oder eine Mitteilung einer Aufsichtsbehörde erhält, die bzw. der sich direkt auf die Datenverarbeitung der gemeinsam genutzten personenbezogenen Daten durch die andere Partei oder auf eine mögliche Nichteinhaltung der Datenschutzgesetze durch die betreffende Partei in Bezug auf die Dienstleistungen bezieht, benachrichtigt die Partei, die die Beschwerde, den Bescheid oder die Mitteilung erhält, die andere Partei unverzüglich, soweit nach geltendem Recht zulässig, und übermittelt dieser die von ihr in diesem Zusammenhang billigerweise angeforderten Informationen.

3.7. Internationale Datenübertragungen

3.7.1. Die Parteien dürfen gemeinsam genutzte personenbezogene Daten nur innerhalb des EWR, des Vereinigten Königreichs oder der Schweiz (je nach Sachlage) oder in anderen Ländern nutzen, die von der Europäischen Kommission, dem ICO oder dem Schweizerischen EDÖB (je nach Sachlage) als einen angemessenen Schutz personenbezogener Daten im Hinblick auf Datenschutz und die Grundrechte und -freiheiten von Personen gewährleistende Länder anerkannt sind.

3.7.2. Wenn eine Partei gemeinsam genutzte personenbezogene Daten in ein Drittland außerhalb des EWR, des Vereinigten Königreichs oder der Schweiz (je nach Sachlage) ohne ein von der Europäischen Kommission, dem ICO oder dem Schweizerischen EDÖB (je nach Sachlage) erklärtes angemessenes Schutzniveau übermittelt oder exportiert, muss sie ihre Pflichten gemäß den Datenschutzgesetzen erfüllen, indem sie (i) angemessene und von den Datenschutzgesetzen als geeignete Schutzmaßnahme anerkannte Übermittlungskontrollmechanismen nutzt oder (ii) die Bedingungen dieser Übermittlung durch die in diesen Vertrag aufzunehmenden Standardvertragsklauseln regelt.

3.7.3. Darüber hinaus setzt die die gemeinsam genutzten personenbezogenen Daten übermittelnde oder exportierende Partei angemessene zusätzliche Maßnahmen um, die entsprechend dem rechtlichen Risiko des Ziellandes angemessen sind

und ein im Wesentlichen gleichwertiges Datenschutzniveau wie, je nach Sachlage, im EWR, im Vereinigten Königreich bzw. in der Schweiz gewährleisten, und macht diese zum Gegenstand dieses Nachtrags.

3.7.4. Soweit sich die die gemeinsam genutzten personenbezogenen Daten übermittelnde oder exportierende Partei auf einen bestimmten gesetzlichen Mechanismus zur Normalisierung internationaler Datenübermittlungen stützt und dieser Mechanismus später geändert, widerrufen oder von einem zuständigen Gericht für ungültig erklärt wird, vereinbaren die Parteien, nach Treu und Glauben zusammenzuarbeiten, um einen geeigneten alternativen, die Übermittlung rechtskonform unterstützenden Mechanismus zu finden.

4. Pflichten einer als Verantwortlicher handelnden Partei

Dieser § 4 gilt für den Fall, dass eine als Verantwortlicher handelnde Partei im Rahmen einer Beziehung zwischen Verantwortlichem und Auftragsverarbeiter handelt.

4.1. Allgemeines

4.1.1. Wenn eine Partei als Verantwortlicher und die andere Partei als Auftragsverarbeiter handelt, so ist Erstere allein und ausschließlich zur Bestimmung der Zwecke und Mittel der Verarbeitung der von der anderen Partei oder über diese erhaltenen personenbezogenen Daten berechtigt und für die Einhaltung und Erfüllung ihrer Pflichten gemäß den Datenschutzgesetzen verantwortlich und muss insbesondere

a) sicherstellen, dass die im Rahmen des Vertrages bereitgestellten oder zugänglich gemachten personenbezogenen Daten korrekt und aktuell sind,
b) nur rechtmäßige Anweisungen zur Verarbeitung personenbezogener Daten geben,
c) sicherstellen, dass sie über eine angemessene Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten verfügt, wie in diesem Nachtrag und/oder dem Vertrag geregelt,
d) sicherstellen, dass den von der Datenverarbeitung betroffenen Personen zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten alle erforderlichen Hinweise zur angemessenen Verarbeitung (allgemein als „Datenschutzhinweise“ oder „Datenschutzrichtlinien“ bezeichnet) zur Verfügung gestellt werden, um die rechtmäßige Verarbeitung (einschließlich der Erhebung und Weitergabe) der personenbezogenen Daten für die im Vertrag und/oder dem Nachtrag geregelten Zwecke zu ermöglichen,
e) sicherstellen, dass, sofern keine andere in den Datenschutzgesetzen enthaltene Rechtsgrundlage die Rechtmäßigkeit der Verarbeitung begründet, alle erforderlichen Einwilligungen der betroffenen Personen in die Verarbeitung eingeholt und aufgezeichnet werden, und im Fall des Widerrufs einer Einwilligung durch eine betroffene Person sicherstellen, dass dies dem Auftragsverarbeiter mitgeteilt wird, und
f) geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus (unter Berücksichtigung von Art, Umfang, Kontext und Zwecken der Verarbeitung) auch im Hinblick auf eine unbefugte oder unrechtmäßige Verarbeitung oder einen versehentlichen Verlust oder eine versehentliche Zerstörung oder Beschädigung solcher personenbezogener Daten ergreifen und unterhalten.

4.1.2. Der Verantwortliche verpflichtet sich, dem Auftragsverarbeiter keine nicht für die Erbringung der Dienstleistungen erforderlichen speziellen Kategorien personenbezogener Daten (beispielsweise Gesundheitsdaten) zu übermitteln.

5. Pflichten einer als Auftragsverarbeiter handelnden Partei

Dieser § 5 gilt für den Fall, dass eine als Auftragsverarbeiter handelnde Partei im Auftrag der anderen Partei handelt. Wenn eine Partei personenbezogene Daten im Auftrag der anderen Partei verarbeitet, muss sie zu diesem Zweck ihre Pflichten gemäß den in den Rechtsordnungen geltenden Datenschutzgesetzen, in denen sie geschäftlich tätig ist, sowie die Pflichten gemäß diesem Nachtrag wie folgt erfüllen:

5.1. Datensicherheit

5.1.1. Der Auftragsverarbeiter wird

a) die von der anderen Partei mitgeteilten und/oder mit ihr vereinbarten Datensicherheitsstandards einhalten,
b) alle personenbezogenen Daten in einer sicheren Umgebung aufbewahren, um sicherzustellen, dass personenbezogene Daten nicht an Dritte weitergegeben (soweit nicht im Rahmen des Vertrages gestattet) oder von Dritten missbraucht werden,
c) in Anbetracht der Art und der Risiken der Datenverarbeitung angemessene Maßnahmen ergreifen, um sicherzustellen, dass es nicht zu einem Datensicherheitszwischenfall kommt, und

d) keine von uns oder anderen Dritten zum Schutz der über die Dienstleistungen zugänglichen Inhalte eingesetzten Technologien umgehen.

5.1.2. Die als Auftragsverarbeiter handelnde Partei verpflichtet sich zur Umsetzung aller geeigneten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten, wobei der Kenntnisstand, die Kosten der Umsetzung und die Art, der Umfang, der Kontext und die Zwecke der Datenverarbeitung sowie die Risiken, der Grad der Wahrscheinlichkeit und die Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen sind, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Insbesondere gilt:

a) Wenn der Händler als Auftragsverarbeiter handelt, ist er zur Umsetzung aller geeigneten technischen und organisatorischen Maßnahmen einschließlich unter anderem der in Anlage 3 geregelten Maßnahmen verpflichtet, um ein angemessenes Sicherheitsniveau für die personenbezogenen Daten zu gewährleisten (einschließlich des Schutzes vor Zerstörung, Verlust oder Änderung auf versehentliche oder unrechtmäßige Weise sowie vor unbefugter Weitergabe oder unbefugtem Zugriff).
b) Soweit Planet als Auftragsverarbeiter handelt, wird Planet die folgenden unter https://www.weareplanet.com/technical-and-organisational-measures abrufbaren und als Übersichtstabelle in Anlage 2 dargestellten technischen und organisatorischen Maßnahmen anwenden.

5.1.3. Ohne Einschränkung der Wesentlichkeit anderer Weitergaben personenbezogener Daten gilt ein Verstoß gegen diese Ziffer 5.1. als wesentliche Vertragsverletzung.

5.2. Vertraulichkeit und Geheimhaltung

5.2.1. Der Auftragsverarbeiter verpflichtet sich zur vertraulichen Behandlung der personenbezogenen Daten, auf die er aufgrund dieses Vertrages zugegriffen hat. Zu diesem Zweck stellt der Auftragsverarbeiter sicher, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder gesetzlichen Vertraulichkeitsverpflichtungen unterliegen und dass seine sämtlichen jeweiligen Mitarbeiter im Hinblick auf ihre jeweiligen Verantwortlichkeiten gemäß den Datenschutzgesetzen geschult sind.

5.3. Anweisungen des Verantwortlichen

5.3.1. Der Auftragsverarbeiter wird die personenbezogenen Daten nur auf schriftliche Anweisung des Verantwortlichen (einschließlich der in diesem Nachtrag dokumentierten Anweisungen) in Verbindung mit den im Rahmen des Vertrages erbrachten Dienstleistungen verarbeiten und darf sie nicht für andere als die in diesem Nachtrag und/oder im Vertrag geregelten Zwecke verwenden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen so schnell wie möglich schriftlich zu informieren, wenn er der Ansicht ist, dass eine Anweisung des Verantwortlichen gegen Datenschutzgesetze verstoßen könnte.

5.4. Unteraufträge

5.4.1. Der Auftragsverarbeiter darf Unterauftragsverarbeiter für die Durchführung von Tätigkeiten im Rahmen dieses Vertrages einsetzen. Ungeachtet dessen kann der Verantwortliche, wenn nach dem Datum dieses Nachtrags neue Unterauftragsverarbeiter vom Auftragsverarbeiter beauftragt werden, aus berechtigten Gründen Einwände gegen einen Wechsel oder die Beauftragung eines neuen Unterauftragsverarbeiters erheben, indem er den Auftragsverarbeiter innerhalb von zehn (10) Tagen nach Bekanntgabe eines neuen Unterauftragsverarbeiters schriftlich benachrichtigt. Wenn keine Einwände erhoben wurden, gilt der Unterauftragsverarbeiter als gebilligt.

5.4.2. Insbesondere erkennt der Händler an, dass die Unterauftragsverarbeiter von Planet für die Erbringung der Dienstleistungen unerlässlich sind und dass, wenn er gegen die Inanspruchnahme eines Unterauftragsverarbeiters durch Planet Einwände erhebt, Planet ungeachtet anderslautender Bestimmungen im Vertrag (einschließlich dieses Nachtrags) nicht verpflichtet ist, dem Händler die Dienstleistung zu erbringen, für die Planet diesen Unterauftragsverarbeiter einsetzt.

5.4.3. Anlage 4 enthält eine Aufstellung der Unterauftragsverarbeiter von Planet und des Händlers, und mit Unterzeichnung dieses Nachtrags ermächtigen Planet und der Händler die jeweils andere Partei zur Inanspruchnahme dieser Unterauftragsverarbeiter.

5.4.4. Der Auftragsverarbeiter schließt mit seinen Unterauftragsverarbeitern eine schriftliche Vereinbarung ab, in der er diesen mit diesem Nachtrag und/oder mit dem Vertrag übereinstimmende Verpflichtungen auferlegt. Wenn ein

Unterauftragsverarbeiter seinen Datenschutzverpflichtungen im Rahmen dieser Vereinbarung nicht nachkommt, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Handlungen und Unterlassungen seines Unterauftragsverarbeiters im selben Umfang, in dem er haften würde, wenn er die betreffende Dienstleistung direkt im Rahmen des Vertrages erbringen würde.

5.4.5. Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigungsklausel, wonach der Verantwortliche für den Fall, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr existiert oder zahlungsunfähig geworden ist, zur Kündigung des Unterauftragsverarbeitungsvertrages berechtigt ist und den Unterauftragsverarbeiter zur Löschung oder Rückgabe der personenbezogenen Daten anweisen kann.

5.5. Unterstützung des Verantwortlichen, Compliance und Audits

5.5.1. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten durch geeignete technische und organisatorische Maßnahmen bei der Bearbeitung von eingehenden Anträgen betroffener Personen. Der Verantwortliche ist berechtigt, den Auftragsverarbeiter jederzeit schriftlich anzuweisen, nicht mehr auf derartige Anträge betroffener Person zu reagieren. Wenn der Auftragsverarbeiter einen Antrag einer betroffenen Person erhält, wird er auf diesen Antrag nach Maßgabe der geltenden Datenschutzgesetze reagieren. Dem Verantwortlichen ist bekannt, dass die Bearbeitung derartiger Anträge betroffener Personen durch den Auftragsverarbeiter im Namen des Verantwortlichen keine Befreiung von den sich aus den einschlägigen Datenschutzgesetzen ergebenden rechtlichen Verpflichtungen und keinen Verzicht auf diese bedeutet.

5.5.2. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen auch bei der Einhaltung der Pflichten gemäß den für die unter diesen Nachtrag fallende Datenverarbeitung relevanten Datenschutzgesetzen einschließlich Meldungen an eine Aufsichtsbehörde oder an betroffene Personen, der Durchführung einer Datenschutzfolgenabschätzung und der vorherigen Konsultation von Aufsichtsbehörden.

5.5.3. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, um die Einhaltung seiner jeweiligen in diesem Nachtrag geregelten Pflichten nachzuweisen, und gestattet und unterstützt auf Verlangen des Verantwortlichen Datenaudits einschließlich Inspektionen.

5.5.4. Der Verantwortliche kann auf eigene Kosten einmal im Jahr mit einer Frist von mindestens 30 Tagen ein Audit zur Bestätigung der Einhaltung der Datenschutzgesetze durchführen. Das Audit wird entweder von einem der Mitarbeiter der Parteien oder von einer unabhängigen, von der auditierenden Partei ausgewählten Stelle durchgeführt, deren unabhängige Mitglieder über die erforderlichen beruflichen Qualifikationen verfügen, zur Vertraulichkeit verpflichtet sind und nicht zu einem Unternehmen gehören, das mit einer der Parteien in Bezug auf die Dienstleistungen in direktem Wettbewerb steht. Die Parteien vereinbaren, dass

a) das Audit sich auf keine finanziellen oder personenbezogenen Daten erstreckt, die sich nicht unmittelbar und ausschließlich auf jede der Parteien, die Sicherheitssysteme und -daten jeder der Parteien potenziell beeinträchtigende Informationen (d. h. Risiken für die Vertraulichkeit von Informationen) sowie den Quellcode von bei der Erbringung der Dienstleistungen verwendeten Computerprogrammen beziehen,
b) der Auditor ohne vorherige Zustimmung keine Dokumente, Dateien, Daten oder Informationen ganz oder teilweise kopieren, fotografieren oder scannen sowie Audio-/Video- oder Computerdateien/-programme erstellen darf und
c) das Audit während der Geschäftszeiten und auf eine Weise durchzuführen ist, die den Betrieb oder die Dienstleistungen der auditierten Partei nicht stört.

5.6. Internationale Datenübertragungen

5.6.1. Der Auftragsverarbeiter darf personenbezogene Daten nur innerhalb des EWR, des Vereinigten Königreichs oder der Schweiz (je nach Sachlage) oder in anderen Ländern verarbeiten, die von der Europäischen Kommission, dem ICO oder dem Schweizerischen EDÖB (je nach Sachlage) als einen angemessenen Schutz personenbezogener Daten im Hinblick auf Datenschutz und die Grundrechte und -freiheiten betroffener Personen gewährleistende Länder anerkannt sind.

5.6.2. Wenn der Auftragsverarbeiter personenbezogene Daten in ein Drittland außerhalb des EWR, des Vereinigten Königreichs oder der Schweiz (je nach Sachlage) ohne ein von der Europäischen Kommission, dem ICO oder dem Schweizerischen EDÖB (je nach Sachlage) erklärtes angemessenes Schutzniveau übermittelt oder exportiert, muss

der Auftragsverarbeiter seine Pflichten gemäß den Datenschutzgesetzen erfüllen, indem er (i) angemessene und von den Datenschutzgesetzen als geeignete Schutzmaßnahme anerkannte Übermittlungskontrollmechanismen nutzt oder (ii) die Bedingungen dieser Übermittlung durch die in diesen Nachtrag aufzunehmenden Standardvertragsklauseln regelt.

5.6.3. Darüber hinaus setzt der Auftragsverarbeiter angemessene zusätzliche Maßnahmen um, die entsprechend dem rechtlichen Risiko des Ziellandes angemessen sind und ein im Wesentlichen gleichwertiges Datenschutzniveau wie, je nach Sachlage, im EWR, im Vereinigten Königreich bzw. in der Schweiz gewährleisten, und macht diese zum Gegenstand dieses Nachtrags.

5.6.4. Soweit sich der Auftragsverarbeiter auf einen bestimmten gesetzlichen Mechanismus zur Normalisierung internationaler Datenübermittlungen stützt und dieser Mechanismus später geändert, widerrufen oder von einem zuständigen Gericht für ungültig erklärt wird, vereinbaren die Parteien, nach Treu und Glauben zusammenzuarbeiten, um einen geeigneten alternativen, die Übermittlung rechtskonform unterstützenden Mechanismus zu finden.

5.7. Datensicherheitszwischenfälle

5.7.1. Wenn der Auftragsverarbeiter von einem Datensicherheitszwischenfall Kenntnis erlangt, der wesentliche Auswirkungen auf die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten hat, hat er den Verantwortlichen unverzüglich zu informieren, jederzeit mit diesem zusammenzuarbeiten und dessen Anweisungen in Bezug auf den betreffenden Datensicherheitszwischenfall zu befolgen, damit dieser eine Untersuchung des Zwischenfalls durchführen, eine angemessene Reaktion formulieren und geeignete weitere Schritte in Bezug auf den Datensicherheitszwischenfall unternehmen kann.

5.7.2. Wenn ein Datensicherheitszwischenfall eintritt oder der Verdacht besteht, dass ein Datensicherheitszwischenfall eingetreten ist oder eintreten könnte, informiert der Auftragsverarbeiter den Verantwortlichen so schnell wie möglich schriftlich mit allen relevanten Informationen über die Einzelheiten des Zwischenfalls, damit der Verantwortliche die Datenschutzgesetze einhalten kann. Zu den relevanten Informationen über den Datensicherheitszwischenfall gehören:

a) Name, Handelsname und mutmaßlich betroffene Informationen,
b) Beschreibung der Art des Zwischenfalls einschließlich nach Möglichkeit der Kategorien und der ungefähren Zahl betroffener Personen,
c) Name und Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters oder einer anderen Kontaktstelle, bei der weitere Informationen eingeholt werden können,
d) Beschreibung der voraussichtlichen Folgen,
e) Beschreibung der vom Auftragsverarbeiter ergriffenen oder zu ergreifenden Maßnahmen für die Behandlung des Zwischenfalls, gegebenenfalls einschließlich Maßnahmen zur Abschwächung seiner möglichen nachteiligen Auswirkungen sowie
f) Kopie des gesamten Schriftverkehrs in diesem Zusammenhang einschließlich des Schriftverkehrs mit allen betroffenen Personen.

5.8. Aufzeichnung der Verarbeitung

5.8.1. Der Auftragsverarbeiter führt schriftliche Aufzeichnungen über alle Kategorien von im Auftrag des Verantwortlichen durchgeführten Datenverarbeitungstätigkeiten, wenn er als Auftragsverarbeiter handelt, darunter:

a) Namen und Kontaktdaten des Verantwortlichen, in dessen Auftrag er handelt, etwaiger weiterer Unterauftragsverarbeiter und gegebenenfalls des Datenschutzbeauftragten,
b) Kategorien der im Auftrag des Verantwortlichen oder der betroffenen Person durchgeführten Datenverarbeitungstätigkeiten,
c) gegebenenfalls Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation einschließlich Angabe dieses Drittlandes oder dieser internationalen Organisation und im Fall von Übermittlungen gemäß den Datenschutzgesetzen,
d) soweit möglich, allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen.

5.9. Rückgabe oder Vernichtung personenbezogener Daten

5.9.1. Nach Erbringung der vertraglich vereinbarten Dienstleistung oder bei Beendigung des Vertrages gibt der Auftragsverarbeiter alle personenbezogenen Daten, auf die er während des Vertragsverhältnisses Zugriff hatte, sowie alle anderen als vertraulich eingestuften Dokumente nach Ermessen des Verantwortlichen zurück und/oder vernichtet diese auf die vom Verantwortlichen angegebene Art und Weise und innerhalb der vom Verantwortlichen angegebenen Fristen, sofern keine gesetzlichen Vorschriften oder Hindernisse ein anderes Vorgehen erfordern.

5.9.2. Ungeachtet dessen werden die personenbezogenen Daten vernichtet, wenn vom Verantwortlichen nicht innerhalb von 3 Monaten nach Erbringung der Dienstleistungen oder Beendigung des Vertrages eine entsprechende Anweisung eingeht. Der Verantwortliche kann vom Auftragsverarbeiter eine schriftliche Bescheinigung über die Vernichtung der vernichteten personenbezogenen Daten und Dokumente verlangen.

5.9.3. Vorbehaltlich der Annahme eines Kostenangebots durch den Verantwortlichen stellt der Auftragsverarbeiter dem Verantwortlichen oder einem von diesem benannten Dritten die personenbezogenen Daten in einem marktüblichen Format zur Verfügung, um die Verarbeitung der personenbezogenen Daten fortzusetzen.

6. Schlussbestimmungen

6.1. Der Nachtrag stellt die gesamte Vereinbarung zwischen Planet und dem Händler in Bezug auf seinen Gegenstand dar und tritt an die Stelle aller gegebenenfalls zwischen den Parteien in Bezug auf diesen Gegenstand getroffenen früheren Vereinbarungen.

6.2. Sofern nicht ausdrücklich durch die Bestimmungen dieses Nachtrags geändert oder ergänzt, bleiben der Vertrag und alle darin enthaltenen Bestimmungen oder die Bestimmungen anderer darin genannter Vereinbarungen oder Dokumente in vollem Umfang in Kraft und wirksam.

6.3. Im Fall eines Widerspruchs der Bestimmungen dieses Nachtrags zu den Bestimmungen einer anderen Änderung oder eines anderen Nachtrags und/oder des Vertrages über die Verarbeitung personenbezogener Daten haben die Bestimmungen dieses Nachtrags Vorrang.

6.4. Das geltende Recht und der Gerichtsstand in Bezug auf diesen Nachtrag richten sich nach dem geltenden Recht und dem Gerichtsstand des Vertrages.

Dieser Nachtrag wird durch Unterzeichnung durch die zeichnungsberechtigten Vertreter der Parteien am eingangs genannten Datum geschlossen.

Planet	**Händler**
Durch: _____	Durch: _____
Name:	Name:
Funktion:	Funktion:

ANLAGE 1

Zwecke der Verarbeitung

Die Parteien sind sich einig, dass Planet personenbezogene Daten (bzw. gemeinsam genutzte personenbezogene Daten) im Namen der betroffenen Person für die folgenden Zwecke verwenden darf:

a) Erfüllung der vertraglichen Pflichten von Planet (beispielsweise um die Verwaltung von Transaktionen zu ermöglichen),
b) Erfüllung der Pflichten gemäß einschlägigen Gesetzen sowie der Anforderungen und Anfragen von Aufsichtsbehörden (beispielsweise zur Überprüfung der Identität der betroffenen Personen),
c) berechtigte Interessen von Planet (beispielsweise zur Verbesserung unseres Feedbacks zu erbrachten Dienstleistungen).

Die Parteien verpflichten sich, personenbezogene Daten (bzw. gemeinsam genutzte personenbezogene Daten) niemals ohne vorherige schriftliche Genehmigung der betroffenen Personen zu verkaufen oder an Dritte weiterzugeben.

Datenschutzrollen

Dienstleistung	Planet	Händler	Datenkategorie und üblicherweise verarbeitete personenbezogene Daten
Gateway	Auftragsverarbeiter	Verantwortlicher	Daten von die Dienstleistungen in Anspruch nehmenden Kunden des Händlers einschließlich: PAN (*primäre Kontonummer*), CVV (*Kartenprüfwert*), Gültigkeitsdatum und Postleitzahl, sofern zu Verifizierungszwecken erforderlich. Bei der APM (*alternative Zahlungsmethode*) wird nur die Kontonummer verarbeitet.
PCI-Proxy	Auftragsverarbeiter	Verantwortlicher	Daten von die Dienstleistungen in Anspruch nehmenden Kunden des Händlers einschließlich: PAN (*primäre Kontonummer*), Gültigkeitsdatum der Karte, CVV (*Kartenprüfwert*).
Erwerb	Verantwortlicher	Verantwortlicher	Daten von die Dienstleistungen in Anspruch nehmenden Kunden des Händlers einschließlich: PAN (*primäre Kontonummer*), CVV (*Kartenprüfwert*), Gültigkeitsdatum und Postleitzahl, sofern zu Verifizierungszwecken erforderlich. Bei der APM (*alternative Zahlungsmethode*) wird nur die Kontonummer verarbeitet.
Gerätemiete	Auftragsverarbeiter	Verantwortlicher	Bestimmte begrenzte Daten des die Dienstleistung in Anspruch nehmenden Kunden des Händlers im Zusammenhang mit den über das Gerät ausgeführten Zahlungsvorgängen einschließlich des Betrags der Vorgänge und des Autorisierungscodes.
Gerätekauf	Auftragsverarbeiter	Verantwortlicher	Bestimmte begrenzte Daten des die Dienstleistung in Anspruch nehmenden Kunden des Händlers im Zusammenhang mit den über das Gerät ausgeführten Zahlungsvorgängen (gegebenenfalls) einschließlich des Betrags der Vorgänge und des Autorisierungscodes.
Währungsumrechnung	Auftragsverarbeiter	Verantwortlicher	Daten des die Dienstleistungen in Anspruch nehmenden Kunden des Händlers einschließlich: IP-Adresse (nur für DCC (*dynamische Währungsumrechnung*)), Karten-BIN (*Bankidentifizierungsnummer*) (erste 6 Ziffern), tokenisierte Kartendaten, Geräteinformationen.
Umsatzsteuererstattung	Verantwortlicher	Auftragsverarbeiter	Daten des die Dienstleistungen in Anspruch nehmenden Kunden des Händlers: einschließlich PAN (*primäre Kontonummer*), CVV (*Kartenprüfwert*), Gültigkeitsdatum und Postleitzahl, sofern zu Verifizierungszwecken erforderlich. Bei der APM (*alternative Zahlungsmethode*) wird nur die Kontonummer verarbeitet.
Software für Geschenkkartenlösungen	Auftragsverarbeiter	Verantwortlicher	Daten des die Dienstleistungen in Anspruch nehmenden Kunden des Händlers: Name, E-Mail-Adresse und Postanschrift (bei Ausstellung einer physischen Geschenkkarte).
Software für den Einzelhandel	Auftragsverarbeiter	Verantwortlicher	Daten des die Dienstleistungen in Anspruch nehmenden Kunden des Händlers einschließlich: Name, E-Mail-Adresse, Telefonnummer, Postanschrift, Anmeldeinformationen des Nutzers (IP-Adresse, Browsertyp), Rechnungsdaten des Nutzers (Kontaktinformationen, letzte vier Ziffern der Kreditkarte und Art der Zahlungsmethode).

ANLAGE 2

Bei Verarbeitung personenbezogener Daten (bzw. gegebenenfalls gemeinsam genutzter personenbezogener Daten) durch Planet gelten die Technischen and Organisatorischen Maßnahmen unter https://www.weareplanet.com/technical-and-organisational-measures, die als Übersichtstabelle abrufbar sind unter:

Kategorie	Unterkategorie	Maßnahme
Sicherheitsprogramme und -richtlinien	Sicherheitsprogramm	Das von Planet unterhaltene und implementierte Sicherheitsprogramm regelt, wie Planet Sicherheit handhabt.
	Datenschutzprogramm	Das von Planet unterhaltene und implementierte Datenschutzprogramm regelt die Art und Weise der Erfassung, Nutzung und Weitergabe personenbezogener Daten.
Risiko- und Asset-Management	Risikobewertungen	Planet betreibt ein proaktives Risikomanagement durch unser Enterprise Risk Management Framework und unser robustes Drei-Linien-Modell.
	Asset-Management	Das von Planet unterhaltene und implementierte Asset-Management-Programm realisiert die angemessene Klassifizierung und Kontrolle der Hardware- und Software-Assets während ihres gesamten Lebenszyklus.
Personalschulung und -kontrollen	Anerkennen von Verantwortung	Alle Mitarbeiter von Planet und unabhängigen Auftragnehmer, die Zugriff auf Daten haben können, einschließlich personenbezogene Daten verarbeitender Mitarbeiter und unabhängiger Auftragnehmer erkennen ihre Verantwortung für Datensicherheit und Datenschutz gemäß den Richtlinien von Planet an.
Schulung und Sensibilisierung	Jährliche Sicherheits- und Datenschutzschulungen	Die Mitarbeiter von Planet absolvieren jährliche Sensibilisierungsschulungen zu den Themen DSGVO, KYC (*Know Your Customer*), AML (*Bekämpfung von Geldwäsche*) und Informationssicherheit.
Netzwerk- und Betriebsmanagement	Richtlinien und Verfahren	Planet setzt Richtlinien und Verfahren für ein Netzwerk- und Betriebsmanagement um. Diese Richtlinien und Verfahren betreffen Härtung, Änderungskontrolle, Aufgabentrennung, Trennung von Entwicklungs- und Produktionsumgebungen, Verwaltung der technischen Architektur, Netzwerksicherheit, Schutz vor Malware, Schutz von Daten bei der Übertragung und im Ruhezustand, Datenintegrität, Verschlüsselung, Prüfprotokolle und Netzwerktrennung.
	Schwachstellenanalysen	Planet führt regelmäßig Schwachstellenanalysen und Penetrationstests für die Systeme und Anwendungen einschließlich der personenbezogene Daten verarbeitenden Systeme und Anwendungen von Planet durch.
Technische Zugriffskontrolle	Zugriffskontrolle	Planet ergreift Maßnahmen zur Verhinderung der Nutzung der Datenverarbeitungssysteme durch Unbefugte.
	Datenzugriffskontrolle	Planet ergreift Maßnahmen zur Sicherstellung, dass zur Nutzung eines Datenverarbeitungssystems berechtigte Personen ausschließlich auf die für ihre Zugriffsrechte zulässigen personenbezogenen Daten zugreifen können und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Kategorie	Unterkategorie	Maßnahme
Physische Zugangskontrolle	Sicherheit von Rechenzentren	Planet nutzt vertrauenswürdige Drittanbieter für das Hosting der Produktionsinfrastruktur von Planet. Planet ist auf diese Dritten für die Überwachung der physischen Zugangskontrollen zu den von ihnen verwalteten Rechenzentren angewiesen.
	Bürosicherheit	Der physische Zugang zu den Planet-Büros wird durch Mechanismen wie Anmeldung von Gästen, elektronische Türschlösser, Alarmsysteme und sichere Lagerräume kontrolliert.
	Audits durch Dritte	Planet prüft Auditberichte Dritter, um sicherzustellen, dass die Dienstleister von Planet angemessene physische Zugangskontrollen für unsere verwalteten Rechenzentren durchführen.
Verfügbarkeitskontrollen	Verfügbarkeit	Planet hat Maßnahmen zur Gewährleistung der sofortigen Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten im Fall eines physischen oder technischen Zwischenfalls umgesetzt.
Offenlegungskontrollen	Offenlegung	Planet setzt Maßnahmen um, mithilfe derer gewährleistet ist, dass personenbezogene Daten während der elektronischen Übertragung, des Transports oder der Speicherung auf Speichermedien (manuell oder elektronisch) nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
Trennungskontrollen	Trennung	Planet setzt Maßnahmen um, mithilfe derer gewährleistet ist, dass für unterschiedliche Zwecke erhobene personenbezogene Daten getrennt verarbeitet werden können.
Zertifizierungen	PCI-Einhaltung	Planet verpflichtet sich, seine Dienstleistungen in Übereinstimmung mit den für unsere Angebote geltenden PCI-DSS-Compliance-Standards zu erbringen.
Verschlüsselung	Verschlüsselungsmechanismen	Planet setzt in verschiedenen Phasen Datenverschlüsselungsmechanismen ein, um das Risiko eines unbefugten Zugriffs auf Daten im Ruhezustand und während der Übertragung zu verringern. Darüber hinaus ist der Zugriff auf kryptografische Schlüsselmaterialien von Planet auf eine ausgewählte Gruppe von autorisierten Mitarbeitern von Planet beschränkt.
Management von Datensicherheitszwischenfällen und -meldung	Zwischenfallmanagement	Planet implementiert ein Programm zum Management von Datensicherheitszwischenfällen, das den Umgang von Planet mit Zwischenfällen regelt.
Datenspeicherung und -löschung	Datenspeicherung	Planet implementiert und unterhält Richtlinien und Verfahren zur Speicherung personenbezogener Daten und überprüft diese Richtlinien und Verfahren bei Bedarf.

ANLAGE 3

In Fällen, in denen Planet als Verantwortlicher und der Händler als Auftragsverarbeiter handelt, ist der Händler verpflichtet, die folgenden technischen und organisatorischen Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, wozu unter anderem die entsprechenden Maßnahmen gehören:

1. Festlegung der Aufgaben und Zuständigkeiten der personenbezogene Daten verarbeitenden Mitarbeiter sowie Unterrichtung der Mitarbeiter über ihre Aufgaben und Zuständigkeiten in Bezug auf die Einhaltung von Datenschutzgesetzen und -vorschriften
2. Festlegung von Rollen und Profilen für die Nutzer der Anwendungen und Systeme, über die personenbezogene Daten verarbeitet werden, in Übereinstimmung mit den festgelegten Funktionen und Verantwortlichkeiten, um jeden unbefugten Zugriff auf personenbezogene Daten oder Ressourcen zu verhindern. Dieses Zugriffskontrollsystem muss geeignete Mechanismen zur Benutzeridentifizierung und -authentifizierung gewährleisten, darunter beispielsweise in regelmäßigen Abständen zurückzusetzende Passwörter, biometrische Daten, Multifaktorauthentifizierung, automatische Sperrung des Nutzers nach einer bestimmten Anzahl erfolgloser Anmeldeversuche
3. Anwendung von Maßnahmen zur Ermöglichung von Pseudonymisierung und Verschlüsselung personenbezogener Daten
4. Einrichtung von Kontroll- und Zugriffsprotokollen für personenbezogene Daten enthaltende Dateien und Datenträger, die auch Mechanismen zur Beschränkung des Zugriffs enthalten müssen
5. Anwendung automatisierter Maßnahmen zur Einschränkung des Zugriffs für nicht autorisierte Nutzer oder nach Ablauf der entsprechenden Speicherfrist, beispielsweise Löschtechniken und Pseudonymisierung von Daten
6. Einführung von Verfahren zur Beschränkung des physischen Zugangs zu den Einrichtungen, in denen sich die Informationssysteme oder physischen Medien befinden
7. Anwendung von Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Dienstleistungen
8. Einführung von Verfahren zur Wiederherstellung personenbezogener Daten im Fall ihrer Vernichtung, ihres Verlusts oder ihrer Veränderung unter Aufsicht und mit Genehmigung des Datenschutzbeauftragten
9. Einführung von Verfahren zur Erkennung, Bewertung und erforderlichenfalls Meldung von die Rechte und Freiheiten der betroffenen Personen potenziell beeinträchtigenden Datensicherheitszwischenfällen
10. Durchführung regelmäßiger Überprüfungen der Einhaltung der Vorschriften sowie Festlegung und Durchführung von Maßnahmenplänen zur Minderung der festgestellten Risiken
11. Anwendung sonstiger geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus

ANLAGE 4

Die Unterauftragsverarbeiter von Planet können eingesehen werden unter: https://www.weareplanet.com/legal/subprocessor-and-service-provider-list

Die Unterauftragsverarbeiter des Händlers sind: