PICTUREPARK

Vereinbarung zur Datenverarbeitung (DPA)

Zuletzt geändert: 28. Februar 2022

Diese Vereinbarung zur Datenverarbeitung (Data Processing Agreement, "DPA") wird zwischen Vision Information Transaction und angeschlossenen Unternehmen („Picturepark“, „wir“, „uns“ oder „unser“; dem Auftragsverarbeiter) und Ihnen (“Kunde”, “Sie”, “Ihr”, “Ihre, “Benutzer”; dem Verantwortlichen) geschlossen. Diese Vereinbarung unterliegt den Bestimmungen der Picturepark Cloud Service-Verträge und ist integrierender Bestandteil andere Picturepark-Verträge.

1. Definitionen

Sämtliche grossgeschriebenen Begriffe, die nicht in dieser DPA definiert werden, besitzen die im Vertrag festgelegte Bedeutung.

“Auftragsverarbeiter”	bezeichnet uns oder eine andere natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (“Processor”).
“Aufsichtsbehörde”	bezeichnet eine staatliche oder staatlich errichtete Regulierungsstelle, die eine Partei rechtlich bindend kontrolliert;
“Autorisierte verbundene Unternehmen”	bezeichnen Ihre verbundenen Unternehmen, denen Sie die Nutzung unserer Dienste unter dem Vertrag erlaubt haben, welche aber selber keinen Vertrag oder Bestellunterlagen gezeichnet haben;
“Datenschutzgesetze”	bezeichnen alle Gesetze und Verordnungen, einschliesslich der Gesetze und Verordnungen der Europäischen Union, des Europäischen Wirtschaftsraums, ihrer Mitgliedstaaten, des Vereinigten Königreichs und der Schweiz, sowie deren Abänderungen, Nachfolge-Gesetzen oder Erneuerungen, die auf die Verarbeitung personenbezogener Daten anwendbar sind, einschliesslich, soweit anwendbar, die Data Protection Act 2018, die Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, die EU-DSGVO, das Schweizer DSG, die UK-DSGVO und alle anwendbaren nationalen Umsetzungsgesetze, Verordnungen und sekundären Rechtsvorschriften, die sich auf die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation beziehen, in ihrer jeweils geänderten, ersetzten oder aktualisierten Fassung, einschliesslich der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) und die Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
“Betroffene Person”	hat die gleiche Bedeutung wie in den Datenschutzgesetzen oder unter jeder gleichwertigen Datenschutzregelung des geltenden Rechts. Ohne das Vorstehende einzuschränken, bedeutet "betroffene Person" im Wesentlichen eine natürliche Person, die das Subjekt von personenbezogenen Daten ist (“Data Subject”);
“Datum des Inkrafttretens”	bezeichnet den 27. Dezember 2022 bzw. das Datum an dem Sie den Vertrag eingegangen sind, sofern dies am oder nach dem 27. September 2021 geschehen ist, oder das in den Bestellunterlagen vereinbarte oder rechtlich erforderliche Datum;
“Dienste”	bezeichnet unseren Cloud Service, technischen Support oder andere Dienstleistungen, die wir Ihnen und Ihren autorisierten verbundenen Unternehmen zur Verfügung stellen;
“DPA”	bezeichnet diese Vereinbarung zur Datenverarbeitung, inklusive der Anhänge A, B und C;
“Eingeschränkter Transfer”	bezeichnet: (i) wenn die EU-DSGVO Anwendung findet, die Übermittlung von personenbezogenen Daten über die Dienste aus dem EWR entweder direkt oder über eine Weiterübermittlung in ein Land oder einen Empfänger ausserhalb des EWR, die nicht auf der Grundlage einer Angemessenheitsbestimmung (“Adequacy Decisions”) der Europäischen Kommission erfolgt; und (ii) wenn die UK-DSGVO gilt, die Übermittlung von personenbezogenen Daten über die Dienste aus dem Vereinigten Königreich entweder direkt oder über eine Weiterübermittlung in ein Land oder einen Empfänger ausserhalb des Vereinigten Königreichs, die nicht auf einer Angemessenheitsbestimmung gemäss Abschnitt 17A des britischen Datenschutzgesetzes 2018 beruht; und iii) die Übermittlung von personenbezogenen Daten über die Dienste aus der Schweiz entweder direkt oder über eine Weiterübermittlung in ein Land oder einen Empfänger ausserhalb des EWR und/oder der Schweiz, die nicht auf einer Angemessenheitsbestimmung der Europäischen Kommission beruht;
“EU-DSGVO”	bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016;
“EWR”	bezeichnet den Europäischen Wirtschaftsraum;

“Interne IT Infrastruktur”	bezeichnet unsere interne IT-Infrastruktur, die für unsere Unternehmenszwecke sowie für die Verarbeitung von Kundendaten zum Zwecke der Erstellung und Speicherung von Sicherungskopien ausgewählter Kundendaten, der Erbringung professioneller Dienstleistungen und des technischen Supports oder des Hostings des Cloud-Dienstes für Proof-of-Concept (POC)-Einsätze mit Kunden oder potenziellen Kunden, das Staging von Kundeninstanzen oder für Produktentwicklungszwecke eingesetzt wird;
“Kundendaten”	bezeichnen alle Dateien, Inhalte, Metadaten, personenbezogene Daten, vertrauliche Informationen und andere Daten, die mithilfe der Dienste gespeichert oder verarbeitet werden, wie von Ihnen als Verantwortlicher beauftragt;
“Personenbezogene Daten”	hat dieselbe Bedeutung wie in den Datenschutzgesetzen oder anderen gleichwertigen anwendbaren Gesetzen für den Datenschutz. Ohne das Vorangehende einzuschränken, bezeichnet der Begriff “personenbezogene Daten” jede Art von Informationen, die verwendet werden können, eine natürliche Person direkt oder indirekt zu identifizieren, insbesondere durch Nennung eines Namens oder einer persönlichen Identifikationsnummer, oder eines oder mehrerer Faktoren die über die physische, physiologische, genetische, mentale, ökonomische, kulturelle oder soziale Identität der natürlichen Person Aufschluss geben können. Personenbezogene Daten gelten als vertrauliche Daten;
“Standard-Vertragsklauseln” oder “SCCs”	bezeichnen: (i) bei Anwendung der EU-DSGVO die Standardvertragsklauseln im Anhang des Durchführungsbeschlusses 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, veröffentlicht unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0914&from=De/, (“**EU SCCs**”); und (ii) in Fällen, in denen die britische Datenschutz-Grundverordnung (UK-DSGVO) gilt, die Standarddatenschutzklauseln, die gemäss Artikel 46 Absatz 2 Buchstabe c oder d der UK DSGVO angenommen wurden und unter https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/ veröffentlicht sind (“**UK SCCs**”); und (iii) für den Fall, dass personenbezogene Daten aus der Schweiz in ein Land ausserhalb der Schweiz oder des EWR übermittelt werden, die EU-SCCs in der gemäss den Leitlinien des Schweizer Datenschutz- und Öffentlichkeitsbeauftragten (“EDÖB”) geänderten Fassung (“**Schweizer SCCs**”);
“Schweizer DSG”	bezeichnet das Schweizerische Bundesgesetz über den Datenschutz (DSG) in der Fassung der AS 1993 1945 sowie nachfolgende Datenschutzgesetze (i.B. das “neue DSG 2022”);
“UK-DSGVO”	bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, wie in britisches Recht umgesetzt aufgrund von Abschnitt 3 der European Union (Withdrawal) Act 2018.
“Unterauftragsverarbeiter”	bezeichnet jeden Dritten (einschliesslich verbundener Unternehmen des Auftragsverarbeiters), der vom Auftragsverarbeiter direkt oder indirekt mit der Verarbeitung von Kundendaten gemäss dieser DPA beauftragt wurde, um Ihnen die vereinbarten Dienste zu erbringen (“Sub-Processor”;
“Verantwortlicher”	bezeichnet Sie oder die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (“Controller”);
“Vertrag”	bezeichnet den zwischen Ihnen und uns geschlossenen Vertrag über die Bereitstellung von Diensten, wie in den Bestellunterlagen definiert;

2. Zweck

2.1 Wir haben der Bereitstellung von Diensten an Sie gemäss den Bestimmungen des Vertrags zugestimmt. Durch die Bereitstellung der Dienste werden wir Kundendaten in Ihrem Auftrag verarbeiten. Kundendaten enthalten in der Regel auch personenbezogene Daten. Beginnend mit dem Datum des Inkrafttretens werden wir diese Kundendaten verarbeiten und schützen, wie in den Bestimmungen dieser DPA und Nachfolgeversionen dieser DPA für die Laufzeit des Vertrags festgelegt wurde.

2.2 Die Parteien werden Massnahmen ergreifen, um sicherzustellen, dass jede natürliche Person, die unter ihrer Autorität handelt bzw. Zugang zu personenbezogenen Daten hat, diese nur auf ihre Anweisung hin verarbeitet, es sei denn, sie ist durch ein Datenschutzgesetz dazu verpflichtet.

3. Geltungsbereich

3.1 Bei der Bereitstellung der im Vertrag festgelegten Dienste werden wir die Kundendaten nur in dem Umfang verarbeiten, wie dies nach den Bestimmungen des Vertrags und Ihren dort und in dieser DPA dokumentierten Anweisungen nötig ist.

4. Pflichten des Auftragsverarbeiters

4.1 Wir dürfen Kundendaten nur im Rahmen der Bestimmungen dieser DPA sammeln und verarbeiten.

4.2 Wir bestätigen, dass wir Kundendaten in Ihrem Auftrag und ausschliesslich auf Ihre dokumentierte Anweisung hin verarbeiten.

4.3 Wir werden Sie umgehend informieren, sobald unserer Meinung nach eine Ihrer Anweisungen zum Verarbeiten von Kundendaten einen Bruch mit den anwendbaren Datenschutzgesetzen darstellt.

4.4 Wir stellen sicher, dass alle unsere Angestellten, Repräsentanten, Vorstände und Auftragnehmer, die mit der Verarbeitung von Kundendaten beschäftigt sind: (i) um die Vertraulichkeit der Kundendaten wissen und vertraglich gebunden sind, deren Vertraulichkeit zu schützen; (ii) angemessen in ihrer Verantwortung als Auftragsverarbeiter geschult sind; (iii) an die Bedingungen dieser DPA gebunden sind.

4.5 Wir implementieren angemessene technische und organisatorische Verfahren zum Schutz der Kundendaten, wobei der gegenwärtige Stand der Technik, Implementierungskosten, sowie Natur, Geltungsbereich, Kontext und Zweck der Datenverarbeitung, wie auch die Risiken gegeben durch die unterschiedliche Eintrittswahrscheinlichkeit und Schwere in ihren möglichen Auswirkungen auf die Rechte und Freiheiten natürlicher Personen entsprechend berücksichtigt werden.

4.6 Wir treffen den möglichen Risiken angemessene technische und organisatorische Sicherheitsmassnahmen. Hierzu gehören unter anderem: (i) die Pseudonymisierung und Verschlüsselung von Kundendaten; (ii) die Fähigkeit, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Verarbeitungssysteme und Dienste sicherzustellen; (iii) die Fähigkeit, im Falle einer physischen oder technischen Störung die Verfügbarkeit und Zugriffsmöglichkeit auf Kundendaten zeitnah wieder herzustellen; (iv) ein Verfahren für das regelmässige Testen, Überprüfen und Auswerten der Effektivität technischer und organisatorischer Massnahmen, um die Sicherheit der Datenverarbeitung sicherzustellen. Durch Verwendung angemessener Sicherheitsmassnahmen begegnen wir den Risiken bei der Verarbeitung, die speziell durch unbeabsichtigte oder unrechtmässige Zerstörung, Verlust, Veränderung, nicht autorisierter Weitergabe oder Zugriff auf transferierte, gespeicherte oder anderweitig verarbeitete Kundendaten auftreten können.

4.7 Die in Anhang B aufgeführten technischen und organisatorischen Massnahmen werden grundsätzlich als minimaler Sicherheitsstandard betrachtet. Sie nehmen zur Kenntnis und erklären sich damit einverstanden, dass die technischen und organisatorischen Massnahmen weiterentwickelt und überprüft werden und dass wir zusätzlich zu den in den Anhängen dieser DPA genannten Verfahren angemessene alternative Massnahmen einsetzen können, sofern diese Massnahmen mindestens gleichwertig mit den in Anhang B aufgeführten technischen und organisatorischen Massnahmen sind und gemäss unseren Verpflichtungen in den Ziffern 4.5 und 4.6 angemessen sind.

4.8 Sie nehmen zur Kenntnis und erklären sich damit einverstanden, dass es für die Bereitstellung der Dienste an Sie nötig sein kann, auf Kundendaten zuzugreifen, um auf technische Probleme oder berechtigte Anfragen reagieren zu können und die korrekte Funktionsweise des Cloud Service sicherzustellen. Sämtliche dieser Zugriffe durch uns sind auf die in Anhang A definierten Zwecke beschränkt.

4.9 Unter Berücksichtigung der Art der Datenverarbeitung und den uns zur Verfügung stehenden Informationen unterstützen wir Sie sofern möglich mittels angemessener technischer und organisatorischer Massnahmen in der Erfüllung Ihrer Pflichten bei der Beantwortung von Anfragen zur Rechtewahrnehmung von betroffenen Personen, sowie der Einhaltung Ihrer Datenschutz-Pflichten bezogen auf die Verarbeitung von Kundendaten.

4.10 Wir bestätigen, dass wir und/oder unsere verbundenen Unternehmen einen Datenschutzbeauftragten benannt haben, sofern dies nach anwendbarem Datenschutzrecht notwendig ist. Der benannte Datenschutzbeauftragte kann unter www.picturepark.com/terms erreicht werden.

5. Pflichten des Verantwortlichen

5.1 Sie erklären und sichern zu, dass Sie sich an die Bestimmungen des Vertrags, an diese DPA und an alle anzuwendenden Datenschutzgesetze halten.

5.2 Sie erklären und sichern zu, dass Sie sämtliche nötigen Einwilligungen und Berechtigungen besitzen, um uns, unseren angeschlossenen Unternehmen und Unterauftragsverarbeiter zu erlauben, entsprechende Rechte und Pflichten gemäss dieser DPA ausüben zu können.

5.3 Sie sind dafür verantwortlich, sich an sämtliche anwendbare Datenschutzgesetze zu halten, inklusive der Anforderungen für die Übermittlung von Kundendaten gemäss dieser DPA und des Vertrags.

5.4 Sämtliche Ihre autorisierten verbundenen Unternehmen, welche die Dienste verwenden, sind ihrerseits verpflichtet, sich an die von Ihnen in dieser DPA eingegangenen Verpflichtungen zu halten.

5.5 Sie implementieren angemessene technische und organisatorische Verfahren zum Schutz personenbezogener Daten, wobei der gegenwärtige Stand der Technik, Implementierungskosten, sowie Natur, Geltungsbereich, Kontext und Zweck der Datenverarbeitung, wie auch die Risiken gegeben durch unterschiedliche die Eintrittswahrscheinlichkeit und Schwere in ihren möglichen Auswirkungen auf die Rechte und Freiheiten natürlicher Personen entsprechend berücksichtigt werden. Sie treffen den möglichen Risiken angemessene technische und organisatorische Sicherheitsmassnahmen.

5.6 Sie nehmen zur Kenntnis und erklären sich damit einverstanden, dass einige Ihrer Anweisungen, inklusive der Zerstörung und Rückgabe von Daten durch uns, unserer Unterstützung bei Inspektionen, Datenschutz-Folgenabschätzungen (DSFA) oder der Bereitstellung jeglicher Unterstützung im Rahmen dieser DPA, zusätzliche Gebühren zur Folge haben können, die nicht unangemessen sein dürfen. In einem solchen Fall werden wir Sie im Voraus über diese Gebühren informieren, sofern nichts anderes vereinbart wurde.

6. Unterauftragsverarbeiter

6.1 Sie nehmen zur Kenntnis und erklären sich einverstanden, dass: (i) unsere angeschlossenen Unternehmen als Unterauftragsverarbeiter eingesetzt werden dürfen; und dass (ii) wir, bzw. unsere angeschlossenen Unternehmen ihrerseits Unterauftragsverarbeiter mit der Erbringung der Dienste beauftragen dürfen.

6.2 Wir werden keinen Unterauftragsverarbeiter ermächtigen, personenbezogene Daten ohne vorherige Benachrichtigung an Sie gemäss 6.4 zu verarbeiten.

6.3 Sämtliche Unterauftragsverarbeiter, die Kundendaten bei der Bereitstellung von Diensten an Sie verarbeiten, sind verpflichtet: (i) sich an unsere in dieser DPA festgelegten Pflichten zu halten; (ii) im Rahmen einer schriftlichen Vereinbarung beauftragt zu werden, welche im Wesentlichen dieselben von uns durchsetzbaren Verpflichtungen enthält wie in dieser DPA ausgeführt; und (iii): wir anerkennen und sind damit einverstanden, dass wir für die Verarbeitung personenbezogener Daten durch einen Unterauftragsverarbeiter zur Erfüllung seiner Verpflichtungen gemäss dieser DPA voll verantwortlich und haftbar sind.

6.4 Sie ermächtigen uns, die in der Liste unter der Adresse www.picturepark.com/terms publizierten Unterauftragsverarbeiter zur Verarbeitung von Kundendaten einzusetzen. Sollte sich die Liste der Unterauftragsverarbeiter, die Kundendaten verarbeiten, während der Laufzeit dieser DPA ändern, werden wir Sie mindestens 30 Tage im Voraus per E-Mail oder Briefpost darüber informieren. Dies geschieht bevor neue oder ersatzweise Unterauftragsverarbeiter Kundendaten in Verbindung mit der Bereitstellung der Dienste verarbeiten.

6.5 Sie haben das Recht, dem Einsatz neuer oder ersatzweiser Unterauftragsverarbeiter zu widersprechen, indem Sie uns umgehend schriftlich innerhalb von zehn (10) Geschäftstagen nach Erhalt unseres Hinweises (siehe Absatz 6.4) informieren. Sollten Sie dem Einsatz eines neuen oder ersatzweisen Unterauftragsverarbeiters widersprechen, ist es Ihnen erlaubt, den Vertrag oder den jeweils gültigen Auftrag in Bezug auf die Dienste, die von uns ohne einen neuen oder ersatzweisen Unterauftragsverarbeiter nicht bereitgestellt werden können, zu kündigen. Wir werden Ihnen alle im Voraus für die betroffenen Dienste bezahlten Gebühren für die verbleibende Laufzeit des Vertrags (bzw. den jeweils gültigen Auftrag) ab dem Folgetag des effektiven Kündigungsdatums rückerstatten.

7. Eingeschränkter Transfer

7.1 Falls es sich um einen eingeschränkten Transfer handelt, vereinbaren die Parteien, dass die Übertragung von Kundendaten von Ihnen an uns oder von uns an einen Unterauftragsverarbeiter, den geltenden SCCs unterliegt.

7.2 Die Parteien vereinbaren, dass die EU-SCCs für eingeschränkte Transfers aus dem EWR gelten sollen. Die EU-SCCs gelten als vertraglich abgeschlossen und durch Verweis in diese DPA inkludiert, und werden wie folgt ausgefüllt und ausgewendet:

(i) Modul Zwei (Übermittlung von Verantwortlichen an Auftragsverarbeiter) gilt, wenn Sie ein Verantwortlicher von Kundendaten sind und wir Kundendaten verarbeiten;

(ii) Modul Drei (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) findet Anwendung, wenn wir Auftragsverarbeiter von Kundendaten sind und wir einen (Unter-)Auftragsverarbeiter zur Verarbeitung der Kundendaten einsetzen;

(iii) In Klausel 7 der EU-SCCs findet die optionale Kopplungsklausel keine Anwendung;

(iv) In Klausel 9 der EU SCCs gilt Option 2, und die Frist für die Mitteilung von Änderungen der Unterauftragsverarbeiter beträgt 30 Tage;

(v) In Klausel 11 der EU-SCCs findet die fakultative Klausel/Definition keine Anwendung;

(vi) In Klausel 17 der EU-SCCs gilt Option 1 und die EU-SCCs unterliegen österreichischem Recht;

(vii) In Klausel 18(b) der EU-SCCs werden Streitigkeiten von den österreichischen Gerichten entschieden;

(viii) Anhang I der EU SCCs gilt mit den in Anhang A dieser DPA enthaltenen Informationen als ausgefüllt;

(ix) Anhang II der EU SCCs gilt mit den in Anhang B dieser DPA enthaltenen Informationen als ausgefüllt.

7.3 Die Parteien vereinbaren, dass die EU SCCs in der in Abschnitt 7.2 geänderten Fassung wie folgt angepasst werden, wenn das Schweizer DSG auf einen eingeschränkten Transfer Anwendung findet:

(i) Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ("EDÖB") ist die alleinige Aufsichtsbehörde für eingeschränkte Transfers, die ausschliesslich dem Schweizer DSG unterliegen;

(ii) Eingeschränkte Transfers, die sowohl dem Schweizer DSG als auch der EU-DSGVO unterliegen, werden von der in Anhang A dieser DPA genannten EU-Aufsichtsbehörde bearbeitet;

(iii) Der Begriff "Mitgliedstaat" darf nicht so ausgelegt werden, dass betroffene Personen in der Schweiz von der Möglichkeit ausgeschlossen werden, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort (Schweiz) gemäss Artikel 18 Buchstabe c der EU-DSGVO einzuklagen;

(iv) Wenn eingeschränkte Transfers ausschliesslich dem Schweizer DSG unterliegen, sind alle Verweise auf die DSGVO in den EU-DSGVO als Verweise auf das Schweizer DSG zu verstehen;

(v) Unterliegen die eingeschränkten Transfers sowohl dem Schweizer DSG als auch der EU-DSGVO, so sind alle Verweise auf die DSGVO in den EU-SCCs als Verweise auf das Schweizer DSG zu verstehen, soweit die eingeschränkten Transfers dem Schweizer DSG unterliegen;

(vi) Die Schweizer SCCs schützen auch die Personendaten von juristischen Personen bis zum Inkrafttreten des revidierten Schweizer DSG.

7.4 Die Parteien vereinbaren, dass die UK SCCs auf die eingeschränkten Transfers aus dem Vereinigten Königreich Anwendung finden. Die UK-SCCs gelten als vertraglich abgeschlossen und durch Verweis in diese DPA inkludiert, und werden wie folgt ausgefüllt und ausgewendet:

(i) Anhang 1 der UK SCCs gilt als mit den in Anhang A dieser DPA aufgeführten Informationen ausgefüllt; und

(ii) Anhang 2 der UK SCCs gilt als mit den in Anhang B dieser DPA aufgeführten Informationen ausgefüllt.

7.5 Sollte eine Bestimmung dieser DPA direkt oder indirekt im Widerspruch zu einer SCCs stehen, so haben die Bestimmungen der anwendbaren SCCs Vorrang vor den Bestimmungen der DPA.

8. Anträge auf Auskunft, Änderung und Löschung von betroffenen Daten

8.1 Sie können während oder nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und/oder Bereitstellung der Kundendaten verlangen. Sie anerkennen und erklären sich damit einverstanden, dass wir die Anfrage bearbeiten und dass wir die Anfrage in Übereinstimmung mit unserem Standardverfahren erfüllen, soweit dies angemessen möglich ist.

8.2 Für den Fall, dass wir eine Anfrage von einer betroffenen Person in Bezug auf Kundendaten erhalten, werden wir die betroffene Person an Sie verweisen, sofern dies nicht gesetzlich verboten ist. Sie erstatten uns angemessene Kosten, die uns durch die gebührende Unterstützung bei der Bearbeitung einer Anfrage einer betroffenen Person entstehen, vorausgesetzt, dass wir Sie vorgängig schriftlich über diese Kosten informieren. Für den Fall, dass wir gesetzlich verpflichtet sind, der betroffenen Person zu antworten, werden Sie in vollem Umfang mit uns kooperieren.

9. Audit

9.1 Wir stellen Ihnen gegen eine angemessene Gebühr sämtliche vernünftigerweise erforderlichen Informationen zur Verfügung, um die Einhaltung unserer Pflichten zur Datenverarbeitung zu belegen sowie Audits oder Inspektionen zu erlauben und zu unterstützen.

9.2 Sämtliche von Ihnen im Rahmen dieser DPA durchgeführten Audits bestehen aus der Überprüfung unserer neuesten Berichte, Zertifizierungen und/oder von Auszügen davon, die durch uns oder einen unabhängigen Prüfer erstellt wurden. Der Prüfer muss dabei Vertraulichkeitsregelungen unterliegen, die mindestens so streng sind, wie die im Vertrag festgelegten. Sollten die so zur Verfügung gestellten Unterlagen Ihrer berechtigten Ansicht nach nicht ausreichend sein, haben Sie das Recht eine umfangreichere Prüfung vorzunehmen, die: (i) auf Ihre Kosten durchzuführen ist; (ii) sich auf im Voraus zu vereinbarende und ausschliesslich Sie betreffende Angelegenheiten bezieht; (iii) während Schweizer Geschäftszeiten und mit angemessenen Vorankündigungsfristen von mindestens vier (4) Wochen stattfindet, sofern keine wesentlichen Einwände dagegen sprechen; und (iv) auf eine Weise durchgeführt wird, die unser Tagesgeschäft nicht beeinträchtigt.

9.3 Dieser Paragraph 9 soll Ihr Recht auf Überprüfung in Übereinstimmung mit anwendbarem Recht nicht einschränken. Sie ist vielmehr dafür gedacht, die Vorgehensweise der darauf basierenden Überprüfungen zu klären.

10. Verletzung des Schutzes personenbezogener Daten

10.1 Wir werden Sie unverzüglich nach Bekanntwerden (und in jedem Fall innert 72 Stunden nach Entdeckung) einer versehentlichen oder unrechtmässigen Zerstörung, eines Verlusts, einer Änderung oder einer unbefugten Offenlegung oder eines unbefugten Zugriffs auf Ihre Kundendaten (**"**Datenschutzverletzung**"**) informieren.

10.2 Wir werden jede Sicherheitsverletzung umgehend untersuchen und die nötigen Massnahmen unternehmen, um die Ursachen zu finden, nachteilige Auswirkungen einzuschränken und eine Wiederholung zu verhindern. Sobald uns nähere Informationen zur Verfügung stehen, erhalten Sie von uns eine Beschreibung der Sicherheitsverletzung, die Art der betroffenen Kundendaten und angemessene weitere Informationen zu den betroffenen Kundendaten, wie sie von Ihnen angemessen angefordert werden.

10.3 Wir werden sämtliche wirtschaftlich angemessenen Massnahmen treffen, um Ihre Kundendaten abzusichern, damit Auswirkungen einer möglichen Datenschutzverletzung möglichst gering ausfallen, und Sie gemäss den rechtlichen Vorgaben darin unterstützen, Ihren Verpflichtungen erwachsend aus anwendbarem Recht nachzukommen.

11. Erfüllung, Kooperation und Beantwortung

11.1 Sollten wir eine Anfrage oder Beschwerde bezüglich der Verarbeitung von Kundendaten erhalten, die negative Folgen für Sie hat, werden wir Sie umgehend darüber informieren, sofern dies nicht durch anwendbares Recht oder eine gerichtliche Anordnung untersagt ist.

11.2 Es ist uns erlaubt, in Übereinstimmung mit rechtlichen oder regulatorischen Anforderungen (inklusive beispielsweise Aufbewahrungsanforderungen), Kopien von Kundendaten anzufertigen und aufzubewahren.

11.3 Wir werden Sie in angemessener Weise bei der Erfüllung Ihrer Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen ("DSFA") unterstützen, unter Berücksichtigung der Art der Verarbeitung und der uns zur Verfügung stehenden Informationen.

11.4 Sie werden uns innerhalb eines angemessenen Zeitraums über Änderungen der Datenschutzgesetze und der anwendbaren Vorschriften informieren, die Auswirkungen auf unsere vertraglichen Pflichten haben können. . Wir werden in einem angemessenen Zeitraum auf daraus womöglich resultierende Änderungen der Bedingungen dieser DPA oder der technischen und organisatorischen Massnahmen zur Aufrechthaltung unserer Einhaltung der Vorschriften reagieren. Sollten wir nicht in der Lage sein, die nötigen Änderungen vorzunehmen, können Sie den Teil oder die Teile der Dienste kündigen, die Anlass für die Nichteinhaltung sind. Sofern andere bereitgestellte Dienste von solchen Änderungen nicht betroffen sind, bleibt die Erbringung dieser Dienste davon unberührt.

11.5 Der Verantwortliche und der Auftragsverarbeiter und so anwendbar deren Vertreter sind auf Anweisung zur Kooperation mit der zuständigen Aufsichtsbehörde verpflichtet, um den in dieser DPA und aus Datenschutzgesetzen erwachsenden Vereinbarungen nachzukommen.

12. Haftung

12.1 Sämtliche im Vertrag festgelegten Haftungsbeschränkungen gelten auch für alle Haftungsansprüche, die durch einen Verstoss gegen die in dieser DPA vereinbarten Bedingungen entstehen sollten.

12.2 Beide Parteien kommen überein, dass wir die Haftung für Verstösse gegen Bedingungen dieser DPA übernehmen, die durch Vorsatz oder Fahrlässigkeit unserer Unterauftragsverarbeiter entstehen, und zwar in gleichem Umfang wie wir haftbar wären, wenn wir die Dienste der Unterauftragsverarbeiter direkt selber gemäss den Bedingungen dieser DPA, bzw. unter Berücksichtigung der im Vertrag getroffenen Regelungen, ausgeführt hätten.

12.3 Beide Parteien kommen überein, dass Sie die Haftung für jegliche Verstösse gegen diese DPA übernehmen, die durch Vorsatz oder Fahrlässigkeit Ihrer autorisierten verbundenen Unternehmen entstehen, als seien diese Handlungen vorsätzlich oder fahrlässig durch Sie selbst begangen worden.

12.4 Sie sind nicht berechtigt, mehr als einmal den gleichen Schaden geltend zu machen.

13. Laufzeit und Beendigung

13.1 Die Laufzeit dieser DPA fällt mit dem Beginn des Vertrags zusammen und endet automatisch mit der Beendigung oder Kündigung des Vertrags.

14. Löschung und Rückgabe von personenbezogenen Daten

14.1 Nach Erhalt Ihrer schriftlichen Aufforderung, die innerhalb von 10 Tagen nach dem Datum des Inkrafttretens der Beendigung des Vertrags bei uns eingeht, werden wir nach Ihrem Wunsch personenbezogene Daten entweder gemäss unseren internen Richtlinien löschen oder an Sie zurückgeben. Wir werden in jedem Fall innerhalb von neunzig (90) Tagen nach Beendigung des Vertrages alle Kundendaten von unseren Systemen löschen und Ihnen auf Anfrage eine Bescheinigung über diese Löschung ausstellen. Ausgenommen von dieser Regelung sind Kundendaten, die auf Storage-Typen oder Backup-Optionen mit längerer Vorhaltezeit gespeichert wurden. Für diese Speicherarten dürfen wir die Daten für die Dauer der vom Hosting-Typ oder der Backup-Option bestimmten Speicherdauer (oder “Retention period”) plus neunzig (90) Tage aufbewahren. Sollten Sie uns anweisen, die Kundendaten vor Ablauf der vorgängig genannten Fristen zu löschen, werden wir die Kundendaten gegen eine angemessene Gebühr ohne schuldhaftes Zögern entfernen, sofern dies nicht durch geltendes Recht untersagt ist.

15. Allgemeines

15.1 Diese DPA stellt die gesamte Abmachung und Absprache zwischen den Parteien in Bezug auf den darin geregelten Gegenstand dar.

15.2 Sollte eine Bestimmung dieser DPA ungültig sein oder werden, so bleiben die rechtlichen Auswirkungen der übrigen Regelungen davon unberührt. Anstelle der unwirksamen Bestimmung gilt dann eine wirksame Bestimmung als vereinbart, die der von den Parteien wirtschaftlich Gewollten am nächsten kommt. Das Gleiche gilt für etwaige Vertragslücken.

15.3 Vorbehaltlich anders lautender Bestimmungen in den SCCs unterliegt diese DPA dem auf den Vertrag anwendbaren Recht. Der ausschliesslich geltende Gerichtsstand für alle aus dieser DPA resultierenden Streitigkeiten ist der im Vertrag festgelegte.

15.4 Die Bestimmungen dieser DPA überdauern die Beendigung anderer relevanter bestehender Verträge und gelten so lange, wie wir im Besitz Ihrer personenbezogenen Daten sind.

15.5 Alle Mitteilungen bezogen auf diese DPA müssen schriftlich erfolgen und per E-Mail an die in den Bestellunterlagen angegebenen E-Mail-Adressen mit Kopie an legal@picturepark.com gesendet werden.

Anhang A

Liste der Parteien, Beschreibung der Verarbeitung und Übermittlung von personenbezogenen Daten, zuständige Aufsichtsbehörde.

MODUL ZWEI:
VON VERANTWORTLICHEN ZUM AUFTRAGSVERARBEITER

A. LISTE DER PARTEIEN

Verantwortlicher bezeichnet **Sie** mit Namen und Adresse wie im Vertrag oder den Bestellunterlagen festgehalten.	
Name der Kontaktperson, Position und Vertragsdetails:	Wie von Ihnen, dem Verantwortlichen, in Ihrem Konto des Cloud Services und/oder in den Bestellunterlagen angegeben, die für Benachrichtigungs- und Rechnungsstellungszwecke verwendet werden.
Tätigkeiten, die für die im Rahmen der SCCs übermittelten Daten relevant sind:	Nutzung der Dienste.
Unterschrift und Datum:	Durch den Abschluss des Vertrags hat der Verantwortliche die SCCs, die in diese DPA per Referenz mitsamt ihren Anhängen inkludiert sind, zum Zeitpunkt des Inkrafttretens des Vertrags automatisch unterzeichnet.
Rolle:	Datenexporteur.
Name des Vertreters (falls zutreffend):	Jeder Vertreter des Vereinigten Königreichs oder der EU, der in Ihrer Datenschutzrichtlinie genannt wird.

Auftragsverarbeiter bezeichnet **uns** (Picturepark) mit folgender Adresse: Vision Information Transaction AG (besser bekannt als “Picturepark”) Industriestrasse 25 CH-5033 Buchs (AG), Schweiz	
Name der Kontaktperson, Position und Vertragsdetails:	Picturepark DPO wie online publiziert unter https://picturepark.com/terms/dpo/.
Tätigkeiten, die für die im Rahmen der SCCs übermittelten Daten relevant sind:	Die Bereitstellung von cloudbasierten Datenverarbeitungs-Lösungen und Dienstleistungen für Sie, in deren Rahmen der Auftragsverarbeiter personenbezogene Daten auf Ihre Anweisung hin gemäss den Bedingungen des Vertrags verarbeitet.
Unterschrift und Datum:	Durch den Abschluss des Vertrags hat der Auftragsverarbeiter die SCCs, die in diese DPA per Referenz mitsamt ihren Anhängen inkludiert sind, zum Zeitpunkt des Inkrafttretens des Vertrags automatisch unterzeichnet.

Rolle:	Datenimporteur
Name des Vertreters (falls zutreffend):	Siehe https://prighter.com/q/15848945763 für unseren aktuellen EU DSGVO oder UK DSGVO Vertreter: EU DSGVO Vertreter: PrighterGDPR-Rep by Maetzler Rechtsanwalts GmbH & Co KG Schellinggasse 3/10 1010 Vienna, Austria https://prighter.com, support@prighter.com Bitte dem gesamten Schriftverkehr den Betreff hinzufügen: ID-15848945763 UK DSGVO Vertreter: PrighterUK-Rep by Prighter Ltd 20 Mortlake Mortlake High Street London, SW14 8JN, United Kingdom https://prighter.com, support@prighter.com Bitte dem gesamten Schriftverkehr den Betreff hinzufügen: ID-15848945763

B. BESCHREIBUNG DER VERARBEITUNG UND DER ÜBERMITTLUNG

Kategorien der betroffenen Personen:	Die von Ihnen autorisierten Benutzer der Dienste, einschliesslich, aber nicht beschränkt auf: • Angestellte, Vertreter, Berater, Consultants, Freiberufler der verantwortlichen Stelle (die natürliche Personen sind). • Benutzer, verbundene Unternehmen und andere Teilnehmer, die von der verantwortlichen Stelle ermächtigt wurden, auf die Dienste zuzugreifen oder sie gemäss den Bedingungen des Vertrags zu nutzen. • Interessenten, Kunden, Klienten, Geschäftspartner und Verkäufer der verantwortlichen Stelle (die natürliche Personen sind) und Personen, mit denen diese Endnutzer per E-Mail und/oder über andere Nachrichtenmedien kommunizieren. • Mitarbeiter oder Kontaktpersonen von Interessenten, Kunden, Klienten, Geschäftspartnern und Verkäufern der verantwortlichen Stelle. • Lieferanten und Dienstleistungsanbieter der verantwortlichen Stelle. • Andere Personen, soweit sie im Rahmen der über die Dienste verarbeiteten Daten, über E-Mails oder deren Anhänge, in Archivinhalten oder anderen Dateien, Datenbanken oder Ähnlichem identifizierbar sind.
Kategorien von personenbezogenen Daten:	Sie als Verantwortlicher können über Ihre autorisierten Nutzer personenbezogene Daten an die Dienste übermitteln, deren Umfang vom Verantwortlichen bestimmt und kontrolliert wird. Zu den personenbezogenen Daten gehören unter anderem: • Persönliche Daten von Benutzern der Dienste, einschliesslich Namen, Rolle, Funktion, E-Mail-Adressen, Benutzername, Kontonummer, eindeutige Identifikatoren. • Personenbezogene Daten, die aus der Nutzung der Dienste durch einen Benutzer abgeleitet werden, wie z. B. statistische Aufzeichnungen, Business-Intelligence-Informationen, IP-Adressen, Namen von Internet-Providern, Geolokalisierungsdaten, Webbrowser-Informationen, URL, URL-Clickstream. • Bilder, Videos, Dokumente, Tonaufnahmen und alle anderen Dateien, die personenbezogene Daten als Inhalt oder in ihren Metadaten enthalten. • Metadaten, Anmerkungen oder andere Informationen sowie alle Daten, die über die Dienste erstellt, gespeichert, verwaltet oder ausgetauscht werden und personenbezogene Daten enthalten können. • E-Mail- und Nachrichteninhalte, die die betroffenen Personen identifizieren

	oder vernünftigerweise zur Identifizierung verwendet werden können. • Metadaten im Zusammenhang mit E-Mail- oder Datenübertragungsaktivitäten über die Dienste, einschliesslich Empfänger, Absender, Datum, Uhrzeit, Betreff etc., die personenbezogene Daten enthalten können. • Daten, die Sie zum Suchen oder Filtern von Inhalten eingegeben haben und die personenbezogene Daten enthalten können. • Informationen, die von Benutzern im Rahmen von Supportanfragen angeboten werden, sowie Daten, die bei der Inanspruchnahme unseres Supports erfasst, gespeichert und verarbeitet werden. • Andere Daten, die der Verantwortliche von Zeit zu Zeit für die Verarbeitung mit den Diensten hinzufügt oder verwaltet.
Sensible Daten:	Der Auftragsverarbeiter benötigt für die Nutzung der Dienste keine besonderen Kategorien von personenbezogenen Daten. Ob und welche besonderen Kategorien personenbezogener Daten gespeichert und verarbeitet werden, hängt ausschliesslich von Ihnen und der Nutzung der Dienste durch Ihre autorisierten Benutzer ab.
Häufigkeit der Verarbeitung und Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden):	Kontinuierlich während der Dauer des Vertrages.
Art der Verarbeitung:	Der Hauptcharakter der Verarbeitung besteht darin, Ihnen als dem für die Verarbeitung Verantwortlichen den Cloud-Dienst und andere Dienste zur Verfügung zu stellen. Die Verarbeitung umfasst unter anderem folgende Vorgänge: • Bereitstellung des Cloud Services über unsere Hosting-Infrastruktur. • Prüfung der Nutzung des Dienstes auf Einhaltung des Vertrags oder des geltenden Rechts. • Analyse der Nutzung des Dienstes und der Kundendaten zum Zweck des Schutzes vor Bedrohungen oder zur Verbesserung der Dienste. • Bereitstellung von technischem Support, Problemdiagnose und Fehlerbehebung, um den effizienten und ordnungsgemässen Betrieb der Systeme zu gewährleisten und technische Probleme sowohl allgemein bei der Bereitstellung des Dienstes als auch speziell bei der Beantwortung von Supportanfragen von Ihnen oder Ihren Benutzern zu identifizieren, zu analysieren und zu beheben. • Information der Benutzer über Änderungen, Probleme oder Wartungsarbeiten im Zusammenhang mit dem Dienst. • Erfüllung Ihrer Anfragen nach professionellen Dienstleistungen oder Audits, die den Zugriff auf und die Verarbeitung von Kundendaten beinhalten. • Erfüllung sonstiger Verpflichtungen, die im Vertrag festgehalten sind.
Zweck(e) der Datenübermittlung und Weiterverarbeitung:	Kundendaten, einschliesslich personenbezogener Daten, werden an Unterauftragsverarbeiter übermittelt, die einen Teil der Daten verarbeiten müssen, um ihre Dienstleistungen für den Auftragsverarbeiter als Teil der vom Auftragsverarbeiter für den Verantwortlichen erbrachten Dienste zu erbringen.
Der Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieses Zeitraums:	Sofern nichts anderes schriftlich vereinbart wurde, gilt dies für die Dauer des Vertrages, vorbehaltlich der Klausel 14 der DPA.
Bei Übermittlungen an (Unter-) Verarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben:	In der Liste der Unterauftragsverarbeiter, die über https://picturepark.com/terms abgerufen werden kann, sind die von den einzelnen Unterauftragsverarbeiter

	verarbeiteten personenbezogenen Daten und die von den einzelnen Unterauftragsverarbeiter erbrachten Dienstleistungen aufgeführt.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) (z. B. gemäss Klausel 13 der SCCs)	• Wenn die EU DSGVO Anwendung findet, dann die Österreichische Datenschutzbehörde. • Wenn die UK DSGVO Anwendung findet, dann die UK Information Commissioner's Office (ICO). • Wenn das Schweizer DSG Anwendung findet, dann der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

MODUL DREI:
VON AUFTRAGSVERARBEITERN AN AUFTRAGSVERARBEITER

A. LISTE DER PARTEIEN

Der **Datenexporteur** sind wir (Picturepark).

Die **Datenimporteure** sind die in der Liste der Auftragsverarbeiter genannten Unterauftragsverarbeiter, die den Namen, die Adresse, die Kontaktdaten und die Tätigkeiten im Zusammenhang mit den an jeden Datenimporteur übermittelten Daten enthält.

B. BESCHREIBUNG DER VERARBEITUNG UND DER ÜBERMITTLUNG

Die Liste der Unterauftragsverarbeiter enthält für jeden Datenimporteur Informationen über die Verarbeitung und Übermittlung der personenbezogenen Daten:

- Kategorien von betroffenen Personen;
- Kategorien von personenbezogenen Daten;
- Art der Verarbeitung;
- Zwecke der Verarbeitung.

Die personenbezogenen Daten werden von jedem Datenimporteur wie folgt verarbeitet:

- auf kontinuierlicher Basis;
- in dem Umfang, der erforderlich ist, um die Dienstleistungen in Übereinstimmung mit dem Vertrag und den Anweisungen des Datenexporteurs zu erbringen;
- für die Dauer des Vertrages und vorbehaltlich der Klausel 14 der DPA.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Die zuständige Aufsichtsbehörde des Datenexporteurs ist:

- Wenn die EU DSGVO Anwendung findet, dann die Österreichische Datenschutzbehörde.
- Wenn die UK DSGVO Anwendung findet, dann die UK Information Commissioner's Office (ICO).
- Wenn das Schweizer DSG Anwendung findet, dann der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

PICTUREPARK

Anhang B:
Technische und Organisatorische Massnahmen

(einschliesslich technischer und organisatorischer Massnahmen zur Gewährleistung der Sicherheit der Daten)

Im Folgenden werden die technischen und organisatorischen Massnahmen beschrieben, die wir zur Gewährleistung eines angemessenen Sicherheitsniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen ergriffen haben.

Gegebenenfalls wird dieser Anhang B als Anhang II zu den SCCs dienen.

Measure	**Beschreibung**
Massnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	Zum Zweck der Übertragungskontrolle werden Verschlüsselungstechnologien eingesetzt. Die Eignung einer Verschlüsselungstechnologie wird am Schutzzweck gemessen. Sofern für die Dienste oder Teile davon nicht anders angegeben, werden Kundendaten, die ausserhalb der gesicherten Netzwerke des Cloud-Dienstes und unserer internen IT-Infrastruktur übertragen werden, oder Kundendaten, die als eingeschränkte Transfers eingestuft werden, durch die Verwendung von Transport Layer Security ("TLS") geschützt (“in transit”). Sofern für die Dienste oder Teile davon nichts anderes angegeben ist, werden Kundendaten im Ruhezustand (“at rest”), die ausserhalb der gesicherten Infrastruktur des Cloud-Dienstes und unserer internen IT-Infrastruktur gespeichert werden, oder Kundendaten im Ruhezustand, die als eingeschränkte Transfers gelten, durch eine AES256-Bit-Verschlüsselung oder eine Verschlüsselung, die einen im Wesentlichen ähnlichen Schutz bietet, geschützt. Backup-Medien wie Tapes, die für die Suisse Safe Backup Option verwendet werden, oder Backups unserer Systeme, die für Unternehmens- oder Betriebszwecke genutzt werden, sind immer mit AES128-Bit-Verschlüsselung verschlüsselt und werden gemäss unseren Backup-Rotations- und Aufbewahrungsplänen kontinuierlich überschrieben. Bitte beachten Sie, dass in den Fällen, in denen Sie "Europa" oder "Schweiz" als Region ausgewählt haben, oder in denen Sie die Suisse Safe Backup Option gewählt haben, die Kundendaten “at rest” ausschliesslich im EWR (einschliesslich der Schweiz) oder in der Schweiz gemäss den Definitionen im Vertrag gespeichert werden. Die Laptops des Unternehmens werden mit AES-256-Verschlüsselung oder ähnlichem verschlüsselt; für die Verwendung anderer Geräte, die auf Kundendaten zugreifen, gelten unsere allgemeinen IT- und Sicherheitsrichtlinien. Der Zugang zu unserer internen IT-Infrastruktur erfordert die Verwendung von sicheren Protokollen wie HTTPS mit SSL/TLS, VPN-Tunneling oder Ähnlichem.
Massnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	Zur Wahrung der Vertraulichkeit und Integrität und soweit dies zum Schutz der Kundendaten auf der Grundlage des Risikos als angemessen erachtet wird, werden die Kundendaten selbst oder die Speichermedien, die Kundendaten enthalten, mit branchenüblichen Verschlüsselungstechnologien versehen. Der Zugang zu den Kundendaten, der für die Durchführung der jeweiligen Aufgabe erforderlich ist, erfolgt nach den Grundsätzen der "geringsten Rechte" (“least privilege”) und des "unbedingten Bedarfs" (“need to know”) und erfordert eine sichere Authentifizierung mit individuellen Benutzerkonten und starken Passwörtern, die stets verschlüsselt sind. Der Zugang zu den Systemen wird durch Sicherheitsgruppen und Zugriffskontrolllisten eingeschränkt. Konten werden nach mehreren fehlgeschlagenen Zugriffsversuchen gesperrt.

	Wenn der Fernzugriff auf eines unserer Systeme für den Cloud Service oder unsere interne Infrastruktur genutzt wird, verwenden wir VPN-Tunnel oder https (SSL/TLS)-gesicherte Verbindungen und eine mehrstufige Authentifizierung. Wo dies möglich ist, wird der Zugang nur vorübergehend gewährt und der Zugriff auf Systeme und Informationen wird protokolliert. Die Verfügbarkeit und Ausfallsicherheit von personenbezogenen Daten und Kundendaten wird durch die Verwendung einer redundanten Infrastruktur, die Spiegelung von Kundendaten oder die Durchführung regelmässiger Sicherungen von Kundendaten aufrechterhalten, was von den Storage-Typen und Backup-Optionen abhängen kann, die Sie für den Cloud Service ausgewählt haben. Darüber hinaus verfügen wir über Notfallwiederherstellungs- und Geschäftskontinuitätspläne, um die nachteiligen Auswirkungen von Katastrophen zu mildern. Die Systeme für die produktive Nutzung unseres Cloud Services sind physisch von unserer internen IT-Infrastruktur getrennt.
Massnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	Wir halten in unserer IT-Infrastruktur eine angemessene Redundanz aufrecht, um die mangelnde Verfügbarkeit oder den Verlust von Kundendaten zu minimieren. Wenn Sie entsprechende Storage-Typen ausgewählt haben, werden die Kundendaten in einem oder mehreren Rechenzentren gespeichert, um die Zerstörung oder den Verlust von Kundendaten zu minimieren und die Dienste so schnell wie möglich wiederherzustellen, wie in unserem Vertrag festgelegt. Wenn Sie die entsprechenden Backup-Optionen ausgewählt haben, können die Kundendaten in zusätzlichen Datenzentren gespeichert werden, wobei Sicherheitsvorkehrungen wie die verschlüsselte Speicherung auf Offline-Backup-Bändern gemäss unserem Vertrag zum Einsatz kommen. Die Backups werden gemäss unseren Backup-Verfahren aufbewahrt. Wir unterhalten einen Notfallwiederherstellungs- und Geschäftskontinuitätsplan, der in regelmässigen Abständen, mindestens jedoch einmal pro Kalenderjahr, überprüft wird.
Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung	Wir führen regelmässig Sicherheitsbewertungen sowie Schwachstellen- und Penetrationstests für unsere Infrastruktur durch, die für die Bereitstellung der Dienste verwendet wird. Wo immer möglich, automatisieren wir das Testing mittels kontinuierlichen Tests und Kontrollen der Testergebnisse bereits während der Entwicklung und bei Releases neuer Versionen des Cloud Service um Sicherheitsprobleme frühzeitig erkennen und beheben zu können. Unsere Testsysteme sind logisch und/oder physisch von unseren produktiven Systemen und Umgebungen getrennt. Wir überprüfen und verbessern regelmässig unsere Sicherheitsrichtlinien.
Massnahmen zur Identifizierung und Autorisierung der Nutzer	Der Zugang zu den Kundendaten, der für die Durchführung der jeweiligen Aufgabe erforderlich ist, erfolgt nach den Grundsätzen der "geringsten Rechte" (“least privilege”) und des "unbedingten Bedarfs" (“need to know”) und erfordert eine sichere Authentifizierung mit individuellen Benutzerkonten und starken Passwörtern, die stets verschlüsselt sind und durchgesetzt werden und regelmässig oder aufgrund von Ereignissen wie dem Rollenwechsel oder der Beendigung des Beschäftigungsverhältnisses von Mitarbeitern geändert werden müssen. Der Zugang zu den Systemen wird durch Sicherheitsgruppen und Zugangskontrolllisten eingeschränkt. Konten werden nach mehreren fehlgeschlagenen Zugriffsversuchen gesperrt. Der Fernzugriff auf die Datenverarbeitungssysteme des Cloud-Dienstes und unsere interne IT-Infrastruktur ist nur über einen sicheren VPN-Tunnel oder über https (SSL/TLS)-gesicherte Verbindungen möglich, wobei eine Multi-Faktor-Authentifizierung zum Einsatz kommt. Zum Schutz unserer verschiedenen IT-Infrastrukturen, die für die Bereitstellung der Dienste verwendet werden, einschliesslich unserer internen IT-Infrastruktur, sind netzspezifische Firewalls vorhanden. Autorisierungsanfragen und -bereitstellungen sowie ausgewählte Benutzeraktivitäten werden protokolliert.
Massnahmen zum Schutz der Daten während der Übermittlung	Sofern für die Dienste oder Teile davon nicht anders angegeben, werden Kundendaten, die ausserhalb der gesicherten Netzwerke des Cloud-Dienstes und unserer internen IT-Infrastruktur übertragen werden, oder Kundendaten, die als

	eingeschränkte Transfers eingestuft werden, durch die Verwendung von Transport Layer Security ("TLS") geschützt (“in transit”). Der Fernzugriff auf die Datenverarbeitungssysteme des Cloud-Dienstes und unserer internen IT-Infrastruktur ist nur über einen sicheren VPN-Tunnel oder über https (SSL/TLS)-gesicherte Verbindungen möglich, wobei eine Multi-Faktor-Authentifizierung vorhanden ist.
Massnahmen zum Schutz der Daten während der Speicherung	Sofern für die Dienste oder Teile davon nichts anderes angegeben ist, werden Kundendaten im Ruhezustand (“at rest”), die ausserhalb der gesicherten Infrastruktur des Cloud-Dienstes und unserer internen IT-Infrastruktur gespeichert werden, oder Kundendaten im Ruhezustand, die als eingeschränkte Transfers gelten, durch eine AES256-Bit-Verschlüsselung oder eine Verschlüsselung, die einen im Wesentlichen ähnlichen Schutz bietet, geschützt. Backup-Medien wie Bänder, die für die Suisse Safe Backup Option verwendet werden, oder Backups unserer Systeme, die für Unternehmens- oder Betriebszwecke genutzt werden, sind immer mit AES128-Bit-Verschlüsselung verschlüsselt und werden gemäss unseren Backup-Rotations- und Aufbewahrungsplänen kontinuierlich überschrieben.
Massnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden	Aufgrund ihrer jeweiligen Sicherheitsanforderungen sind unser Firmengebäude und das Rechenzentrum unserer internen IT-Infrastruktur in verschiedene Sicherheitszonen mit unterschiedlichen Zugangsberechtigungen unterteilt. Die CCTV-Überwachung erfolgt rund um die Uhr. Die für die Bereitstellung unseres Cloud-Service genutzten Rechenzentren entsprechen den baulichen und inhaltlichen Sicherheitsstandards und -anforderungen für Rechenzentren, die mindestens nach ISO 27001 zertifiziert sind. Ausgenommen hiervon ist unsere interne IT-Infrastruktur, für die im Wesentlichen vergleichbare Anforderungen gelten, ohne dass derartige Zertifizierungen bescheinigt werden müssen.
Massnahmen zur Gewährleistung der Protokollierung von Ereignissen	Verschiedene sicherheitsrelevante Ereignisse der Systeme und der Infrastruktur für die Bereitstellung unserer Dienste werden protokolliert, überwacht und bei Bedarf analysiert. Für den Zugang zu Systemen und Netzen müssen sich die Nutzer authentifizieren, und jeder erfolgreiche oder erfolglose Zugriffsversuch wird bei einem zentralisierten Dienst oder auf dem entsprechenden System protokolliert. Die Protokolle werden in der Regel für mehrere Monate oder für einen Zeitraum aufbewahrt, der für den betreffenden Dienst auf der Grundlage seiner Datenverarbeitungsklassifizierung als angemessen erachtet wird, um eine rückwirkende Sicherheitsüberprüfung zu ermöglichen und den Datenschutzanforderungen zu entsprechen.
Massnahmen zur Gewährleistung der Systemkonfiguration, einschliesslich der Standardkonfiguration	Wo immer möglich, basiert unsere Systemkonfiguration auf unseren internen Vorlagen, Images oder Containern, die Konfigurationen nach den besten Praktiken der Branche (“best practises”) und unter Nutzung von erweiternden Sicherheitssystemen zur Verbesserung des Betriebssystems verwenden. Bevor Konfigurationen oder Codeänderungen auf Produktionssysteme angewendet werden, durchlaufen diese Konfigurationen oder dieser Code strenge Qualitätskontrollprozesse auf physisch oder logisch getrennten QA-Systemen (Test- oder Staging-Systemen). Ausgenommen hiervon sind Notfälle, in denen wir vernünftigerweise beschliessen, Änderungen sofort anzuwenden, um potenzielle oder tatsächliche negative Auswirkungen von Sicherheitsvorfällen abzumildern.
Massnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	Die Mitarbeiter sind angewiesen, Kundendaten nur im Rahmen und für die Zwecke ihrer Aufgaben zu erheben, zu verarbeiten und zu nutzen, z. B. bei der Bereitstellung von technischem Support auf der Grundlage von Supportanfragen oder ausgewählten Professional Services. Alle Kundendaten müssen gemäss unseren allgemeinen IT- und Sicherheitsrichtlinien oder anderen dokumentierten Sicherheits- und Datenschutzanweisungen verarbeitet werden. Unsere IT- und Sicherheitsrichtlinien und -verfahren werden regelmässig überprüft und verbessert, um den besten Praktiken der Branche und den einschlägigen Standards (“best practises”) zu entsprechen.

Massnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	Wir nutzen ausschliesslich Drittanbieter für Infrastructure-as-a-Service ("IaaS") oder Platform-as-a-Service (“PaaS”) für die Bereitstellung unseres Cloud Services mit Rechenzentren, die über aktuelle ISO 27001-Zertifizierungen und optional: SSAE 16 SOC 1 Typ II oder SOC 2 Attestation Reports verfügen, oder die über andere im Wesentlichen gleichwertige Zertifizierungen und/oder Bescheinigungen verfügen. Auf Ihre schriftliche Anfrage hin (höchstens einmal innerhalb eines Zeitraums von 12 Monaten) stellen wir Ihnen innerhalb eines angemessenen Zeitraums eine Kopie der zuletzt abgeschlossenen Zertifizierungs- und/oder Bescheinigungsberichte zur Verfügung (sofern dies die Sicherheit der Dienste insgesamt nicht beeinträchtigt). Jeder Auditbericht, der Ihnen als für die Verarbeitung Verantwortlicher vorgelegt wird, wird als vertrauliche Information behandelt und unterliegt den im Vertrag definierten Vertraulichkeitsbestimmungen. Von der Bescheinigung der Zertifizierung ausgenommen ist unsere interne IT-Infrastruktur, für die ähnliche Anforderungen gelten, ohne dass eine Bescheinigung dieser Zertifizierungen erforderlich ist. Unsere IT- und Sicherheitsrichtlinien sowie unsere Softwareentwicklungsprozesse werden regelmässig überprüft und verbessert, um den besten Praktiken der Branche und den einschlägigen Standards (“best practises”) zu entsprechen.
Massnahmen zur Gewährleistung der Datenminimierung	Wenn die Kundendaten für die Zwecke, für die sie verarbeitet wurden, nicht mehr benötigt werden, werden sie gemäss den Aufbewahrungsrichtlinien (“retention policies”) in dieser DPA und unserem Vertrag mit Ihnen gelöscht. Wo immer möglich, werden die Kundendaten bei jeder Löschung zunächst nur gesperrt und dann mit einer gewissen Verzögerung endgültig gelöscht. Dies geschieht, um versehentliche oder möglicherweise absichtliche Löschungen eines Dritten zu verhindern. Die Datensammlung beschränkt sich auf den Zweck der Verarbeitung (bzw. auf die Daten, die der Kunde zur Verfügung stellt). Interne Sicherheitsvorkehrungen sorgen dafür, dass nur das Mindestmass an Zugang gewährt wird, welches für die Ausführung der erforderlichen Funktionen notwendig ist. Wir beschränken den Zugang zu den Kundendaten auf die an der Verarbeitung beteiligten Parteien nach dem Grundsatz des "unbedingten Bedarfs" (“need to know”) und unter Anwendung von differenzierten Zugangsprofilen.
Massnahmen zur Gewährleistung der Datenqualität	Alle verarbeiteten Kundendaten werden von Ihnen, dem Verantwortlichen, bereitgestellt. Wir bewerten nicht die Qualität der von Ihnen bereitgestellten Kundendaten. Wir bieten integrierte Funktionen im Cloud-Service, die Ihnen helfen, die Qualität der von Ihnen gespeicherten Kundendaten zu verstehen und zu überprüfen. Unser Cloud-Service ist so konzipiert, dass die Datenintegrität durch mehrere Prüfungen auf Anwendungs- und Systemebene sichergestellt wird. Unser kontinuierlicher Testprozess stellt sicher, dass der Cloud-Service wie vorgesehen funktioniert, bevor er in unserer Produktionsumgebung eingesetzt wird.
Massnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung	Wir verwenden ein Datenklassifizierungsschema für alle von uns gespeicherten Kundendaten, in dem auch die Standardaufbewahrungsfristen (“retention periods”) für Daten festgelegt sind. Wenn Kundendaten gelöscht werden, werden sie dauerhaft aus unseren aktiven Systemen und Datenbanken entfernt, gegebenenfalls mit einer gewissen Verzögerung nach der ersten Sperrung. Kundendaten können in Sicherungskopien oder anderen Sicherungsspeichern aufbewahrt werden, bis sie durch neuere Sicherungskopien ersetzt oder gemäss den im Vertrag und dieser DPA festgelegten Aufbewahrungsfristen gelöscht werden.
Massnahmen zur Gewährleistung der Rechenschaftspflicht	Wir überprüfen unsere IT- und Sicherheitsrichtlinien intern nach Bedarf und mindestens einmal pro Jahr, um sicherzustellen, dass sie immer noch relevant sind, den besten Praktiken der Branche entsprechen und befolgt werden. Alle Mitarbeiter, auch Auftragnehmer, die mit Kundendaten umgehen, müssen unsere internen IT- und Sicherheitsrichtlinien anerkennen. Für Mitarbeiter, die sich nicht an diese Richtlinien halten, gibt es disziplinarische oder rechtliche Sanktionen. Die Mitarbeiter werden mindestens einmal pro Jahr bzgl. unseren IT- und Sicherheitsrichtlinien oder anderen geltenden Richtlinien geschult. Datenschutz-Folgenabschätzungen (“data protection impact assessments”) sind fester Bestandteil jeder neuen Initiative zur Datenverarbeitung, z. B. bei der Bewertung neuer Unterauftragsverarbeiter (oder der von Zeit zu Zeit erforderlichen

	Neubewertung bestehender Unterauftragsverarbeiter) und bei wesentlichen Änderungen von Datenverarbeitungsprozessen und -systemen.
Massnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	Der Cloud-Dienst verfügt über integrierte Funktionen, mit denen Sie Kundendaten exportieren und löschen können. Wir stellen auch eine API zur Verfügung, auf welche die Benutzer mit CRUD-Aktionen für alle wichtigen Entitätstypen von Kundendaten zugreifen können. Darüber hinaus bieten wir Ihnen Dienstleistungen für standardisierte Exporte von Kundendaten zu vordefinierten Bedingungen an, wie in unserem Vertrag definiert (Verhinderung eines "Lock-in"). Wenn Ihre Nutzung des Cloud-Dienstes beendet wird, löschen wir die Kundendaten in Übereinstimmung mit unseren Aufbewahrungsrichtlinien (“retention periods”), wie sie im Vertrag und in der DPA definiert sind.
Massnahmen, die der (Unter-) Auftragsverarbeiter ergreifen muss, um dem Verantwortlichen (und bei Übermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter den Datenexporteur) unterstützen zu können.	Die Weitergabe von Kundendaten an Dritte erfolgt grundsätzlich nur bei Vorliegen einer entsprechenden Vereinbarung und nur für die konkret benannten Zwecke. Beim Übermitteln von Kundendaten ausserhalb des EWR stellen wir sicher, dass am Zielort bzw. in der Zielorganisation ein angemessenes Datenschutzniveau gemäss den Datenschutzanforderungen der Europäischen Union und anderen anwendbaren Vorschriften besteht, z.B. durch Verträge auf der Grundlage der EU SCCs.