PICTUREPARK

# Vereinbarung zur Datenverarbeitung (DPA)

Zuletzt geändert: 30. März 2021

Diese Vereinbarung zur Datenverarbeitung (Data Processing Agreement, "DPA") wird zwischen Vision Information Transaction und angeschlossenen Unternehmen („Picturepark“, „wir“, „uns“ oder „unser“; dem Datenprozessor) und Ihnen (“Kunde”, “Sie”, “Ihr”, “Ihre, “Benutzer”; dem Datencontroller) 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.

| | |
|---|---|
| **“Vertrag”** | bezeichnet den zwischen Ihnen und uns geschlossenen Vertrag über die Bereitstellung von Diensten, wie in den Bestellunterlagen definiert; |
| **“Autorisierte verbundene Unternehmen”** | bezeichnet Ihre verbundenen Unternehmen, denen Sie die Nutzung unserer Dienste unter diesem Vertrag erlaubt haben, welche aber selber keinen Vertrag oder Bestellunterlagen gezeichnet haben; |
| **“Datencontroller”** | 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 (Verantwortliche); |
| **“Kundendaten”** | bezeichnet alle Dateien, Inhalte, Metadaten, personenbezogene Daten, vertrauliche Informationen und andere Daten, die mithilfe der Dienste gespeichert oder verarbeitet werden, wie von Ihnen als Datencontroller beauftragt; |
| **“Datensubjekt”** | hat die gleiche Bedeutung wie in den Datenschutzgesetzen oder unter jeder gleichwertigen Datenschutzregelung des geltenden Rechts. Ohne das Vorstehende einzuschränken, bedeutet "Datensubjekt" im Wesentlichen eine natürliche Person, die das Subjekt von personenbezogenen Daten ist; |
| **“Datenschutzgesetze”** | bezeichnet 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); |
| **“DPA”** | bezeichnet diese Vereinbarung zur Datenverarbeitung, inklusive der Anhänge A, B und C; |
| **“Datum des Inkrafttretens”** | bezeichnet den 1. Juli 2021 bzw. das Datum an dem Sie den Vertrag eingegangen sind, sofern dies nach dem 1. Juli 2021 geschehen ist, oder das in den Bestellunterlagen vereinbarte Datum; |
| **“EU-DSGVO”** | bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016; |
| **“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; |

| | |
|---|---|
| **“Datenprozessor”** | bezeichnet uns oder eine andere natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Auftragsverarbeitende). |
| **“Dienste”** | bezeichnet unseren Cloud Service, technischen Support oder andere Dienstleistungen, die wir Ihnen und Ihren autorisierten verbundenen Unternehmen zur Verfügung stellen; |
| **“Standard-Vertragsklauseln” oder “SCC”** | bezeichnet die Standard-Vertragsklauseln zur Übermittlung personenbezogener Daten an Datenprozessoren in Drittländern gemäss c2010-593 - Entscheidung 2010/87EU (wie im Anhang C ausgeführt; inklusive nachfolgender Änderungen und Nachfolge-Gesetzen); |
| **“Subprozessor”** | bezeichnet natürliche oder juristische Personen, die von uns oder einem unserer verbundenen Unternehmen mit der Verarbeitung von Kundendaten beauftragt wurden, um Ihnen die vereinbarten Dienste zu erbringen; |
| **“Schweizer DSG”** | bezeichnet das Schweizerische Bundesgesetz über den Datenschutz (DSG) in der Fassung der AS 1993 1945; |
| **“UK-DSGVO”** | bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, wie in britisches Recht umgesetzt. |

## 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 Datenprozessors

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 Datenprozessor 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 Werden Kundendaten eines Datensubjekts der EU (oder des Vereinigten Königreichs oder der Schweiz) ausserhalb des Europäischen Wirtschaftsraumes ("EWR"; oder ausserhalb des Vereinigten Königreichs oder der Schweiz) transferiert, dürfen diese nur in Übereinstimmung mit den Standard-Vertragsklauseln verarbeitet werden, ausser die Verarbeitung: (i) findet in einem Drittland oder einem Territorium statt, dessen Datenschutzvorschriften von der EU-Kommission als angemessen sicher eingestuft wird; oder die (ii) von einer Organisation in einem Land erfolgt, welches über andere rechtlich anerkannte und angemessen Sicherheitsmassnahmen verfügt.

4.10 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 Datensubjekten, sowie der Einhaltung Ihrer Datenschutz-Pflichten bezogen auf die Verarbeitung von Kundendaten.

4.11 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 Datencontrollers

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 Subprozessoren 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 den Transfer 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. Subprozessoren

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

6.2 Wir werden keinen Subprozessoren ermächtigen, personenbezogene Daten ohne vorherige Benachrichtigung an Sie gemäss 6.5 zu verarbeiten.

6.3 Sämtliche Subprozessoren, die bei der Bereitstellung von Diensten an Sie, Kundendaten verarbeiten, sind verpflichtet, sich an unsere in dieser DPA festgelegten Pflichten zu halten. Wir anerkennen und sind einverstanden damit, dass wir für die Verarbeitung personenbezogener Daten durch einen Subprozessor zur Erfüllung seiner Verpflichtungen gemäss dieser DPA voll verantwortlich und haftbar sind.

6.4 Sie erklären sich damit einverstanden, dass Subprozessoren personenbezogene Daten zum Zweck der Erbringung der Dienstleistungen für Sie in Länder ausserhalb des EWR transferieren dürfen, sofern dies in Übereinstimmung mit dieser DPA erfolgt. Befinden sich Subprozessoren ausserhalb des EWR, so bestätigen wir, dass diese Subprozessoren: (i) sich in einem Drittland oder Territorium befinden, dessen Sicherheitsniveau von der EU-Kommission als angemessen sicher eingestuft wurde; oder (ii) sich uns gegenüber zur Einhaltung der Standardvertragsklauseln verpflichtet hat; oder (iii) andere rechtlich anerkannte Sicherheitsmassnahmen getroffen hat.

6.5 Sie ermächtigen uns, die von uns beim Datum des Inkrafttretens bereits beauftragten Subprozessoren einzusetzen und wir werden Ihnen die aktuelle Liste der Subprozessoren unter der Adresse www.picturepark.com/terms zur Verfügung stellen. Hierin enthalten sind die Identitäten der Subprozessoren, sowie die entsprechenden Standortländer. Sollte sich die Liste der Subprozessoren, 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 Subprozessoren Kundendaten in Verbindung mit der Bereitstellung der Dienste verarbeiten.

6.6 Sie haben das Recht, dem Einsatz neuer oder ersatzweiser Subprozessoren zu widersprechen, indem Sie uns umgehend schriftlich innerhalb von zehn (10) Geschäftstagen nach Erhalt unseres Hinweises (siehe Absatz 6.5) informieren. Sollten Sie

dem Einsatz eines neuen oder ersatzweisen Subprozessors 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 Subprozessor 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. Transfer der Daten

7.1 Wenn der Datenprozessor im EWR, im Vereinigten Königreich oder in der Schweiz ("Europäische Territorien") ansässig ist und personenbezogene Daten der EU, des Vereinigten Königreichs oder der Schweiz in oder aus Einrichtungen in einem Drittland verarbeitet, gelangen die Standardvertragsklauseln ("SCC") per Verweis in dieser DPA zur Anwendung. Die Parteien vereinbaren, dass der Datenprozessor der Datenimporteur und der Datencontroller der Datenexporteur sind. Sofern die Parteien nichts anderes vereinbaren, gelten die Anhänge A und B dieser DPA für die SCCs, und für die Zwecke der Klauseln 9 und 11(3) der SCCs gilt das Recht des Landes, in dem der jeweilige Datencontroller seinen Sitz hat. Nichts in dieser DPA ist so auszulegen, dass ein Vorrang einer widersprüchlichen Klausel gegenüber den Standardvertragsklauseln begründet wird. Jede Partei anerkennt, dass sie die Möglichkeit hatte, die Standardvertragsklauseln zu lesen. Insbesondere anerkennt der Datenprozessor seine Verpflichtungen: (i) Den Datencontroller gemäss Klausel 5(a) der Standardvertragsklauseln unverzüglich darüber zu informieren, falls er nicht in der Lage ist, die Standardvertragsklauseln einzuhalten; (ii) den Datencontroller gemäss Klausel 5(d)(i) der Standardvertragsklauseln über ein rechtsverbindliches Offenlegungsersuchen einer Strafverfolgungsbehörde zu informieren; und (iii) alle Anfragen des Datencontrollers bezüglich der Verarbeitung, die Gegenstand des Transfers ist, unverzüglich gemäss Klausel 5(e) der Standardvertragsklauseln zu bearbeiten.

7.2 Für den Fall, dass die Europäische Kommission einen Nachfolgesatz von Standardvertragsklauseln ("neue SCCs") genehmigt oder die Behörden des Vereinigten Königreichs einen Satz von Standardvertragsklauseln ("UK SCCs") erlassen, treten automatisch diese neuen SCCs und die UK SCCs durch Verweis in dieser DPA anstelle der zuvor genehmigten SCCs in Kraft. In diesen Fällen gelten die in den Anhängen A und B dieser DPA aufgeführten Informationen als in die entsprechenden Absätze der Neuen SCC und der UK SCC inkludiert, und anerkennt der Datenprozessor die gleichwertigen Verpflichtungen in diesen neuen SCC und UK SCC. Soweit die neuen SCCs oder UK SCCs den Einschluss zusätzlicher Informationen erfordern, die nicht durch die Anhänge A und B dieser DPA abgedeckt sind, kann der Datencontroller diese durch eine schriftliche Mitteilung an den Datenprozessor in die Neuen SCCs und UK SCCs inkludieren lassen.

7.3 Dieser Absatz gilt für den Fall, dass der Datenprozessor in den Europäischen Territorien ansässig ist und einen Subprozessoren in einem Drittland mit der Verarbeitung von personenbezogenen Daten aus der EU, der Schweiz oder dem Vereinigten Königreich beauftragt. In diesem Fall unterstützt der Datenprozessor den Datencontroller und seine verbundenen Unternehmen, die in den europäischen Ländern ansässig sind und/oder die personenbezogene Daten von betroffenen Personen in den europäischen Ländern verarbeiten, dabei, ein angemessenes Schutzniveau für personenbezogene Daten aus der EU, der Schweiz oder dem Vereinigten Königreich zu erreichen, indem er im Namen des Datencontrollers Standardvertragsklauseln mit diesem Subprozessor abschliesst. Der Datencontroller bevollmächtigt hiermit den Datenprozessor für den alleinigen Zweck des Abschlusses solcher Standardvertragsklauseln in seinem Namen. Der Datenprozessor wird dem Datencontroller auf Anfrage unverzüglich Kopien aller gemäss diesem Absatz abgeschlossenen Standardvertragsklauseln zur Verfügung stellen.

## 8. Berichtigung, Löschung und Bereitstellung

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 einem betroffenen Datensubjekt 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 eines Datensubjektes entstehen, vorausgesetzt, dass wir Sie vorgängig schriftlich über diese Kosten informieren. Für den Fall, dass wir gesetzlich verpflichtet sind, dem Datensubjekt 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. Datenschutzverletzungen

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 Datencontroller und der Datenprozessor 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 in der Vereinbarung 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 Subprozessoren entstehen, und zwar in gleichem Umfang wie wir haftbar wären, wenn wir die Dienste der Subprozessoren 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.

13.2 Nach Erhalt Ihrer schriftlichen Aufforderung, die innerhalb von 10 Tagen nach dem Datum des Inkrafttretens der Beendigung der Vereinbarung bei uns eingeht, werden wir nach Ihrem Wunsch personenbezogene Daten entweder gemäss unserer 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.

## 14. Allgemeines

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

14.2 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.

14.3 Vorbehaltlich anders lautender Bestimmungen in den Standardvertragsklauseln 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.

14.4 14.4 Die Bestimmungen dieser DPA überdauern die Beendigung anderer relevanter bestehender Verträge und gelten so lange, wie wir im Besitz Ihrer personenbezogenen Daten sind.

14.5 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:
# Überblick über die von uns durchgeführte Datenverarbeitung

## 1. Datencontroller

Sie als Datencontroller verpflichten sich, die Dienste so nutzen, bzw. Ihren Nutzern Zugriff auf den Cloud Service zu gestatten, wie in den Bedingungen des Vertrags bezüglich der Übertragung der in den untenstehenden Absatz 3, 4 und 5 beschriebenen Kundendaten festgelegt, soweit die im Absatz 6 genannten Formen der Datenverarbeitung davon betroffen sind.

## 2. Datenprozessor

Wir als Datenprozessor erhalten von Ihnen die in den Absätzen 3, 4 und 5 angegebenen Daten, soweit diese für die im Absatz 6 genannten Arten der Datenverarbeitung benötigt werden.

## 3. Datensubjekte

Sie nehmen zur Kenntnis und erklären sich damit einverstanden, dass die Kategorien der Datensubjekte, die Kundendaten mittels dem Cloud Service nutzen und verarbeiten können, ausschliesslich [durch Sie und] die Verwendung des Cloud Service durch Ihre Benutzer bestimmt wird. Ungeachtet des Vorstehenden betrifft die Verarbeitung von Kundendaten üblicherweise die folgenden Kategorien von Datensubjekten:

- Ihre Angestellten, sowie von Ihnen engagierte Freelancer und andere Vertragsnehmer.
- Benutzer, Ihre autorisierten verbundenen Unternehmen und andere Teilnehmer.
- Ihre Partner, Lieferanten und Dienstleister.
- Ihre Kunden oder Ihre Medienkontakte.
- Alle Personen, denen Sie in Übereinstimmung mit den Bestimmungen des Vertrags Zugriff auf die Dienste gewährt haben.
- Andere Personen, soweit Sie den Cloud Service benutzen oder sich dafür registriert haben, oder soweit sie über Inhalte in Dateien oder Metadaten, welche von unseren Diensten verarbeitet werden, identifizierbar sind.

## 4. Kategorien von Kundendaten

Welche Kundendaten verarbeitet werden, wird ausschliesslich durch Verwendung der Dienste durch Sie oder Ihre Benutzer bestimmt. Wird der Cloud Service als registrierter Benutzer verwendet, wird der vollständige Name des Benutzers, sowie dessen Email-Adresse, Passwort und IP-Adresse benötigt. Kundendaten können in Datenbankeinträgen, Metadaten oder Dateien im Dateisystem gespeichert werden, anhand derer Datensubjekte identifiziert werden, oder die auf angemessene Weise für deren Identifikation benutzt werden können.

Bei Benutzung des Cloud Service erklären Sie sich einverstanden und nehmen zur Kenntnis und sind Sie damit einverstanden, dass Sie und Ihre Benutzer sich strikt an die Nutzungsbedingungen (AUP) halten, und dass Kundendaten einschliesslich personenbezogener Daten ausschliesslich mit schriftlicher Einwilligung der Datensubjekte über den Cloud Service verarbeitet werden dürfen.

## 5. Spezielle Kategorien personenbezogener Daten

Wir erfordern für die Nutzung der Dienste keine speziellen Kategorien personenbezogener Daten wie beispielsweise Daten von Kindern. Ob und welche speziellen Kategorien personenbezogener Daten gespeichert und verarbeitet werden, hängt ausschliesslich von der Nutzung der Dienste durch Sie und Ihre Benutzer ab.

## 6. Art der Datenverarbeitung

Die Kundendaten werden grundsätzlich wie folgt verarbeitet:

Kundendaten werden in Übereinstimmung mit dem Vertrag und Ihren Anweisungen verarbeitet, soweit dies für die Bereitstellung der Dienste notwendig ist. Wir prozessieren Daten nur wie von Ihnen als Datencontroller beauftragt.

Arten der Verarbeitung sind unter anderem (aber nicht ausschliesslich):

- Bereitstellung des Cloud Service über unsere Hosting-Infrastruktur.
- Auditierung der Verwendung des Cloud Service, um die Einhaltung des Vertrags bzw. bestehenden Rechts sicherzustellen.
- Das Analysieren der Nutzung des Cloud Service und der Kundendaten zum Zwecke des Schutzes gegen Bedrohungen oder zur Verbesserung des Cloud Service.
- Die Bereitstellung technischen Supports, die Diagnose möglicher Vorfälle und die Beseitigung von Defekten, um sicherzustellen, dass der Cloud Service effizient und reibungslos funktioniert und um technische Probleme zu identifizieren, analysieren und beseitigen, sowohl allgemein für den Betrieb des Cloud Service wie auch im Besonderen, um die Support-Anfragen von Ihnen und Ihren Benutzern beantworten zu können.
- Die Information der Benutzer über Änderungen, Probleme oder Wartungsarbeiten bezüglich des Cloud-Dienstes.
- Die Erfüllung Ihres Auftrags zur Lieferung von Dienstleistungen oder Audits, für welche der Zugriff auf oder die Verarbeitung von Kundendaten notwendig ist.
- Die Erfüllung anderer Verpflichtungen, die sich aus dem Vertrag ergeben.

Sämtliche oben genannten Arten der Verarbeitung beziehen sich auf alle Aspekte und Kategorien von verarbeiteten Kundendaten.

PICTUREPARK

# Anhang B:
# Technische und organisatorische Sicherheitsmassnahmen

Die folgenden Beschreibungen geben einen Überblick über die eingesetzten technischen und organisatorischen Sicherheitsmassnahmen. Hierbei sollte allerdings beachtet werden, dass detaillierte Beschreibungen im Kontext der Datensicherheit möglicherweise nicht zur Verfügung gestellt werden können, um die Integrität der Sicherheitsmassnahmen nicht zu gefährden. Sie nehmen zur Kenntnis und erklären sich einverstanden, dass die hier beschriebenen technischen und organisatorischen Sicherheitsmassnahmen, sowie unsere internen IT-Sicherheitsrichtlinien ausschliesslich nach unserem Ermessen von Zeit zu Zeit aktualisiert und erweitert werden können. Ungeachtet des Vorstehenden werden die technischen und organisatorischen Sicherheitsmassnahmen in keiner materiellen, benachteiligenden Weise geringer ausfallen als die in unseren IT-Sicherheitsrichtlinien (IT Security Policy) beschriebenen Massnahmen.

## 1. Hosting-Infrastruktur

Für die Bereitstellung des Cloud Service verwenden wir die Hosting-Dienste von Drittanbietern in Form von Datencentern und Infrastructure-as-a-Service (IaaS), die nach aktuellem ISO 27001-Standard zertifiziert sind und optional auch ISO 27017- oder ISO 27018-Zertifizierungen aufweisen.

Sofern für die Dienste oder Teile davon nicht anders angegeben, verwenden wir keine Datencenter von Drittanbietern oder IaaS Anbieter für das Hosting unseres Cloud Service, die nicht über die zuvor genannten Zertifizierungen und/oder Bescheinigungen oder über gleichwertige Zertifizierungen und/oder entsprechende Prüfbescheinigungen verfügen.

Ausgenommen hiervon ist unsere interne IT-Infrastruktur, die für Dienste wie Backups, POC, Staging, Tests oder Projektimplementierung verwendet wird und für die im Wesentlichen ähnliche Anforderungen gelten, ohne dass eine Bescheinigung über solche Zertifizierungen erforderlich ist.

## 2. Physische Zugangskontrolle

Technische und organisatorische Massnahmen zur Zugangskontrolle, insbesondere die Legitimierung autorisierter Personen:

**Der Zweck der Zugangskontrolle besteht darin, zu verhindern, dass nicht autorisierte Personen physischen Zugriff auf Einrichtungen zur Datenverarbeitung erhalten, die Kundendaten verarbeiten.**

Wir setzen Massnahmen ein, die sicherstellen sollen, dass unautorisierte Personen keinen Zugriff auf die Einrichtungen zur Datenverarbeitung erhalten, die wir für die Dienste nutzen.

Für unseren Cloud Service richten sich die baulichen und materiellen Sicherheitsstandards nach den Vorgaben für Datencenter, die zumindest nach aktuellem ISO 27001-Standard zertifiziert sind, und optional auch ISO 27017- oder ISO 27018-Zertifizierungen aufweisen.

Ausgenommen hiervon ist unsere interne IT-Infrastruktur, die für Dienste wie Backups, POC, Staging, Tests oder Projektimplementierung verwendet wird und für die im Wesentlichen ähnliche Anforderungen gelten, ohne dass eine Bescheinigung über solche Zertifizierungen erforderlich ist.

## 3. Zugangskontrolle auf Systemebene

Technische und organisatorische Massnahmen bezüglich der Identifizierung und Authentifizierung von Benutzern:

**Der Zweck der Zugangskontrolle auf Systemebene besteht darin, die nicht autorisierte Verwendung von Einrichtungen zur Datenverarbeitung von Kundendaten zu verhindern.**

Abhängig von den jeweils beauftragten Diensten werden folgende Kontrollmechanismen ggf. zusammen mit anderen Massnahmen angewandt: Authentifizierung anhand eines Passworts und/oder Zwei-Faktor-Authentifizierung, dokumentierte Authentifizierungsprozesse und Change-Management-Prozesse, sowie die Protokollierung der Zugriffe auf verschiedenen Ebenen.

Für alle Dienste gilt: (i) Zugriffe auf Systeme zur Datenspeicherung oder -verarbeitung werden protokolliert; (ii) Logischer Zugriff auf die Zentren zur Datenspeicherung und -verarbeitung ist durch den Einsatz von VLAN/VPN beschränkt und geschützt; (iii) Es werden zentralisierte Systeme zur Protokollierung und Alarmierung, sowie Firewalls eingesetzt.

## 4. Zugangskontrolle für Daten

Technische und organisatorische Massnahmen in Bezug auf das Autorisierungskonzept, der Zugriffsrechte auf Daten, sowie das Monitoring und die Aufzeichnung dieser:

**Massnahmen in Bezug auf die Zugriffskontrolle für Daten werden so durchgeführt, dass nur auf solche Daten zugegriffen werden kann, für die auch eine Zugriffsberechtigung existiert und dass Daten während der Verarbeitung und nach der Speicherung nicht auf unberechtigte Weise gelesen, kopiert, verändert oder gelöscht werden können.**

Auf Kundendaten kann nur durch korrekt autorisierte Mitarbeiter zugegriffen werden. Der direkte Zugriff auf Datenbank-Abfragen ist eingeschränkt, Applikationsrechte sind vorhanden und werden erzwungen. Muss für die Durchführung einer bestimmten Aufgabe auf Daten zugegriffen werden, wird der Zugriff innerhalb des Systems und der Applikationen über ein entsprechendes Rollen- und Autorisierungskonzept abgesichert.

## 5. Kontrolle der Datenübertragung

Technische und organisatorische Massnahmen in Bezug auf den Transport, den Transfer, den Versand, die Speicherung und nachfolgende Überprüfungen von Kundendaten auf Datenmedien (manuell oder elektronisch).

**Eine Kontrolle der Datenübertragung ist implementiert, so dass Kundendaten nicht ohne entsprechende Autorisierung gelesen, kopiert, verändert oder gelöscht werden können, während der Übertragung oder wenn auf Datenmedien gespeichert. Dies geschieht so, dass überwacht und sichergestellt wird, dass der Transfer von Kundendaten nur an bestimmte Empfänger bestimmt ist.**

Sofern für die Dienste oder Teile davon nicht anders angegeben, werden Datenübertragungen ausserhalb der Cloud Service-Umgebung oder unserer internen IT-Infrastruktur, die für Dienste wie Backups, POC, Staging, Tests oder Projektimplementierung verwendet wird, verschlüsselt oder auf verschlüsselten Medien gespeichert. Backup-Datenträger wie Tapes für die Suisse Safe Backup Option werden immer verschlüsselt.

Per E-Mail oder über Messaging-Dienste verschickte Kommunikationsinhalte (inklusive der Absender- und Empfängeradressen) können unverschlüsselt übertragen werden. Sollten Sie sich entscheiden, Nachrichten oder Daten mit uns über solche E-Mail- oder Messagingdienste auszutauschen oder Teile des Cloud Service zu nutzen, welche auf der Nutzung solcher E-Mail oder Messaging Dienste basieren, liegt die Verantwortung für mögliche Auswirkungen Ihres Entscheides ausschliesslich bei Ihnen.

Der Transfer von Kundendaten an eine Drittpartei (z.B. Subprozessor) wird nur für einen spezifischen Zweck durchgeführt und wenn eine entsprechende Vereinbarung existiert. Werden Kundendaten an Firmen transferiert, die sich ausserhalb des Europäischen Wirtschaftsraumes (EWR; oder ausserhalb des Vereinigten Königreichs oder der Schweiz) befinden, stellen wir sicher, dass am Zielort oder bei der Zielorganisation ein angemessenes Datenschutzniveau, gemäss den Zusicherungen dieser DPA existiert. Dies geschieht beispielsweise durch die Verwendung von Verträgen basierend auf den Standard-Vertragsklauseln.

Kundendaten, die nur für interne Zwecke, z.B. als Teil der jeweiligen Kundenbeziehung verwendet werden, dürfen nur unter Berücksichtigung der vertraglichen Vereinbarungen und angemessenen Anforderungen an die Datenschutzbestimmungen solcher Drittparteien transferiert werden.

## 6. Kontrolle der Dateneingabe

Technische und organisatorische Massnahmen bezüglich der Aufzeichnung und Überwachung der Umstände der Dateneingabe zum Zweck einer nachträglichen Überprüfung.

**Kontrollen zur Dateneingabe werden verwendet, um eine nachträgliche Überprüfung zu ermöglichen.**

Systemeingaben werden in Form von Logdateien und Datenbankeinträgen aufgezeichnet, wodurch nachträglich überprüft werden kann, ob und durch wen Kundendaten eingegeben, verändert oder gelöscht wurden.

## 7. Kontrolle von Datenbackups und Datenverfügbarkeit

Technische und organisatorische Massnahmen im Bezug auf (physikalische/logische) Daten-Backups:

**Kontrollen von Datenbackups und Datenverfügbarkeit werden eingesetzt, um die Kundendaten vor unvorhersehbarer Zerstörung oder Verlust zu schützen.**

Haben Sie einen entsprechenden Hosting-Typ oder Backup-Option gemäss den vertraglichen Definitionen ausgewählt, so werden wie im Vertrag definiert regelmässig Backups von den Daten unseres Cloud Service angefertigt. Es liegt ausschliesslich in Ihrer Verantwortung, die entsprechenden Optionen auszuwählen, damit Ihnen Datenbackups und die Kontrolle über die Verfügbarkeit von Kundendaten angemessen zur Verfügung stehen.

Backup-Medien, die ausserhalb der Hosting-Infrastruktur des Cloud Service oder unserer internen IT-Infrastruktur für Dienste wie Backups, POC, Staging, Tests oder Projektimplementierung transferiert werden, werden immer verschlüsselt, ausser wir werden von Ihnen anders beauftragt, wofür Sie in diesem Fall verantwortlich sind.

## 8. Kontrolle der Datenverarbeitung

Technische und organisatorische Massnahmen zur Unterscheidung der Kompetenzen von Datencontroller und Datenprozessor.

**Die Kontrolle der Datenverarbeitung soll sicherstellen, dass Kundendaten in Übereinstimmung mit den Anweisungen des Datencontrollers von einem bevollmächtigten Datenprozessoren verarbeitet werden.**

Details zur Kontrolle der Datenverarbeitung sind im Vertrag und der DPA festgelegt.

## 9. Separierung von Daten

Technische und organisatorische Massnahmen bezüglich der Sammlung und separierten Verarbeitung von Daten:

**Kundendaten aus unseren verschiedenen Kunden-Umgebungen werden auf unseren Systemen, bzw. denen unserer Subprozessoren durch technische und organisatorische Massnahmen voneinander separiert.**

Angestellte werden angewiesen, Kundendaten nur im Rahmen der in unseren IT & Security-Sicherheitsbestimmungen definierten und für die Erfüllung Ihrer Pflichten (z.B. die Lieferung von Dienstleistungen) zu sammeln und zu verarbeiten und diese Kundendaten zu löschen, sobald sie für die Bereitstellung von Diensten nicht mehr gebraucht werden, oder sie durch zwingende gesetzliche Vorschriften dazu verpflichtet sind.

Die mittels unserem Cloud Service verarbeiteten Kundendaten werden so gespeichert, dass sie logisch von anderen Kundendaten getrennt sind.

PICTUREPARK

# Anhang C:
# Standard-Vertragsklauseln (SCC)

**BESCHLUSS DER KOMMISSION (2010)593**
**STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)**

gemäss Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

…… ("Daten**exporteur**")

und

…… („Daten**importeur**")

(die „Partei", wenn eine dieser Organisationen gemeint ist, die „Parteien", wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1
**Begriffsbestimmungen**

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1];
b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;
c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;
d) der „Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschliesslich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;
e) der Begriff „anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;
f) die „technischen und organisatorischen Sicherheitsmassnahmen" sind die Massnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmässigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmässigen Verarbeitung schützen sollen.

Klausel 2
**Einzelheiten der Übermittlung**

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3
**Drittbegünstigtenklausel**

[1] Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.
(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.
(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.
(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4
**Pflichten des Datenexporteurs**

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschliesslich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstösst;
b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;
c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmassnahmen;
d) die Sicherheitsmassnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmässigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmässigen Verarbeitung geschützt sind;
e) er für die Einhaltung dieser Sicherheitsmassnahmen sorgt;
f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;
g) er die gemäss Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschliesst, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;
h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmassnahmen zur Verfügung stellt; ausserdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäss den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;
i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäss Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und
j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5
**Pflichten des Datenimporteurs[2]**

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

[2] Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;
c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmassnahmen ergriffen hat;
d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;
   ii) jeden zufälligen oder unberechtigten Zugang und
   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäss bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;
f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;
g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmassnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;
h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;
i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;
j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6
**Haftung**

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.
(2) Ist die betroffene Person nicht in der Lage, gemäss Absatz 1 gegenüber dem Datenexporteur wegen Verstosses des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

    Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoss beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäss den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstosses des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7
**Schlichtungsverfahren und Gerichtsstand**

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

   a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8
**Zusammenarbeit mit Kontrollstellen**

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.
(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Masse und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäss dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.
(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäss Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Massnahmen zu ergreifen.

Klausel 9
**Anwendbares Recht**

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

Klausel 10
**Änderung des Vertrags**

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11
**Vergabe eines Unterauftrags**

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss[3]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.
(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäss Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäss Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.
(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäss Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: …
(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12
**Pflichten nach Beendigung der Datenverarbeitungsdienste**

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.
(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Massnahmen zur Verfügung stellen.

[3] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

Klausel 13
**Sonstiges**

(1) Diese Standardvertragsklauseln haben Vorrang vor allen anderen Vereinbarungen zwischen den Parteien, unabhängig davon, ob diese vor oder nach dem Datum des Abschlusses dieser Standardvertragsklauseln getroffen wurden.