

PIX4D-DATENVERARBEITUNGSVEREINBARUNG

Letzte Änderung: Oktober 2021

Diese Datenverarbeitungsvereinbarung und ihre Anhänge (zusammen die „**DW**“) sind eine Vereinbarung zwischen Ihnen und Pix4D (Pix4D und Sie werden jeweils als „**Partei**“ und gemeinsam als die „**Parteien**“ bezeichnet), die in Verbindung mit der Endnutzer-Lizenzvereinbarung (die „**EULA**“) die Verarbeitung der personenbezogenen Kundendaten in Ihrem Namen durch Pix4D regelt. Diese DWV ist in die EULA eingebunden und bildet einen integralen Bestandteil derselben.

Pix4D kann diese DWV von Zeit zu Zeit aktualisieren. Die auf unserer Website pix4d.com/legal erhältliche Fassung ist die jeweils aktuelle Fassung.

Neben den in dieser DWV definierten Begriffen gelten für diese DWV die definierten Begriffe aus der EULA. Um Zweifel auszuräumen, wird festgestellt, dass alle Verweise auf die EULA diese DWV (einschließlich ihrer Anlagen und der EU SCC wie hierin definiert) und, im anzuwendenden Umfang, Pix4Ds Allgemeine Geschäftsbedingungen für Kunden (die „**Allgemeinen Bedingungen**“) und diesen beigefügte eventuelle Zusatzbedingungen, die in Verbindung mit der Nutzung eines bestimmten Angebots Anwendung finden können (die „**Zusatzbedingungen**“).

INHALTSVERZEICHNIS

PRÄAMBEL	2
1. INKRAFTTRETEN UND LAUFZEIT	2
2. ANWENDUNGSBEREICH DES DATENSCHUTZRECHTS	2
3. DATENVERARBEITUNG UND ROLLEN DER PARTEIEN	2
4. ERSUCHEN DER BETROFFENEN PERSONEN	4
5. PIX4D-PERSONAL	4
6. UNTERAUFTRAGSVERARBEITER	4
7. DATENSICHERHEIT	5
8. DATENÜBERMITTLUNGEN IN NICHT AUF EINER WHITELIST GEFÜHRTE LÄNDER	6
9. VERLETZUNGEN DES SCHUTZES DER DATEN	7
10. STAATLICHE ERSUCHEN UM AUSKUNFT ÜBER DATEN	7
11. ÜBERPRÜFUNG UND AUDIT DER EINHALTUNG VON BESTIMMUNGEN	8
12. BEURTEILUNGEN DER AUSWIRKUNGEN UND KONSULTATIONEN	8
13. RÜCKGABE ODER LÖSCHUNG VON DATEN	8
14. HAFTUNGSBESCHRÄNKUNG	8
15. VERSCHIEDENES	9
16. ANWENDBARES RECHT – BEILEGUNG VON STREITIGKEITEN	10
17. ZUSÄTZLICHE BESTIMMUNGEN FÜR KALIFORNISCHE PERSONENBEZOGENE INFORMATIONEN	10
18. DEFINITIONEN	10

PRÄAMBEL

- A. Die Parteien haben die EULA gemäß den Allgemeinen Bedingungen und den Zusatzbedingungen, wie jeweils anwendbar, geschlossen.
- B. Im Kontext der Erfüllung der EULA können Pix4D und/oder verbundene Unternehmen von Pix4D Zugriff auf personenbezogene Kundendaten haben, die von Ihnen (oder auf Ihre Anweisung) oder von den autorisierten Nutzern mittels der lizenzierten Angebote im Rahmen der EULA offengelegt oder anderweitig zur Verfügung gestellt werden.
- C. Insoweit als Pix4D diese personenbezogenen Kundendaten als Ihr Auftragsverarbeiter verarbeiten wird, möchten die Parteien sicherstellen, dass diese Verarbeitung mit Einklang mit den einschlägigen Datenschutzgesetzen erfolgt, und bestimmte Bedingungen vereinbaren, die für diese Verarbeitung gelten, so wie in dieser DVV festgelegt.

Daher vereinbaren die Parteien nun das Folgende:

1. INKRAFTTRETEN UND LAUFZEIT

- 1.1. **Inkrafttreten.** Diese DVV tritt in Kraft und ersetzt alle zuvor geltenden Datenverarbeitungsvereinbarungen mit dem Wirksamkeitsdatum der Bedingungen (wie nachstehend definiert).
- 1.2. **Laufzeit.** Unabhängig davon, ob die EULA gekündigt wurde oder abgelaufen ist, bleibt diese DVV (einschließlich der P-C-Klauseln wie anwendbar) in Kraft bis, und läuft automatisch ab wenn, Pix4D alle Kundendaten so wie in dieser DVV beschrieben löscht.

2. ANWENDUNGSBEREICH DES DATENSCHUTZRECHTS

- 2.1. **Anwendung der Datenschutzgesetze.** Die Parteien erkennen an, dass europäisches Datenschutzrecht und, je nach Sachlage, außereuropäischer Datenschutz auf die Verarbeitung von personenbezogenen Kundendaten durch Pix4D Anwendung findet.
- 2.2. **Anwendung der Bestimmungen dieser DVV.** Diese DVV wurde speziell für die Zwecke des europäischen Datenschutzrechts abgefasst, aber berücksichtigt auch, soweit möglich, die Vorgaben des außereuropäischen Datenschutzes, insbesondere des CCPA wie in Abschnitt festgelegt, soweit anwendbar. Sofern in dieser DVV nicht anderweitig festgelegt, finden die Bestimmungen dieser DVV unabhängig davon Anwendung, ob europäisches Datenschutzrecht oder außereuropäisches Datenschutzrecht auf die Verarbeitung personenbezogener Kundendaten Anwendung findet.

3. DATENVERARBEITUNG UND ROLLEN DER PARTEIEN

- 3.1. **Rollen der Parteien.** Soweit europäisches Datenschutzrecht Anwendung findet, erkennen die Parteien an und vereinbaren, dass in Bezug auf die Verarbeitung personenbezogener Kundendaten im Kontext der Erfüllung der EULA in Bezug auf (i) die autorisierten Nutzer der lizenzierten Angebote, für die Sie deren Konten verwalten (und insbesondere entscheiden, wer und in welchem Ausmaß Zugriff auf die Organisation hat) und/oder (ii) sonstige Drittparteien, die in den Inhalten erscheinen, die Pix4D mittels der lizenzierten Angebote im Rahmen der EULA offengelegt oder anderweitig zur Verfügung gestellt werden, Sie der Verantwortliche sind und Pix4D der in Ihrem Namen tätige Auftragsverarbeiter

ist.

- 3.2. **Weitere Verarbeitung durch Pix4D.** Ungeachtet des obigen Abschnitts *¡Error! No se encuentra el origen de la referencia.* stimmen Sie zu, dass Pix4D personenbezogene Daten über seine Rolle als Auftragsverarbeiter hinaus verarbeiten darf, nämlich als ein Verantwortlicher für seine eigenen Zwecke in den folgenden Fällen:
- (a) im Hinblick auf die personenbezogenen Daten autorisierter Nutzer der lizenzierten Angebote, einschließlich von Nutzungsdaten, insoweit dies erforderlich ist, um die lizenzierten Angebote zu betreiben (z. B. zu Rechnungszwecken) und anderweitig die EULA zu erfüllen oder seine Rechte auszuüben; konkret für Nutzungsdaten, so lange wie (a) diese Nutzung zu statistischen, analytischen und sonstigen nicht mit bestimmten natürlichen Personen in Beziehung stehende Zwecke erfolgt, und (b) alle eventuellen Informationen, die Drittparteien (außer Pix4Ds einer Vertraulichkeitspflicht unterliegenden Dienstleistern) zur Verfügung gestellt werden, (i) keine identifizierbaren personenbezogenen Daten autorisierter Nutzer enthalten und (ii) keine identifizierbaren personenbezogenen Daten über Sie enthalten; dort, wo (a) und (b) nicht zutreffen, werden wir nicht anonymisierte Nutzungsdaten nur insoweit für Nutzungsanalysen und Produktverbesserungszwecke nutzen, wie Sie dieser Verarbeitung in Ihren Datenschutzeinstellungen für Ihr persönliches Konto zugestimmt haben.
 - (b) im Hinblick auf personenbezogene Daten von Dritten, die in den Inhalten erscheinen, welche Pix4D mittels der lizenzierten Angebote offengelegt oder anderweitig für seine eigenen Zwecke als Verantwortlicher zur Verfügung gestellt werden, solange (a) diese Nutzung für statistische, Forschungs- und Entwicklungs-, Vergleichs- und sonstige, nicht mit bestimmten natürlichen Personen in Beziehung stehende Zwecke erfolgt und (b) ggf. Dritten (außer Pix4Ds einer Vertraulichkeitspflicht unterliegenden Dienstleistern) zur Verfügung gestellte Informationen (i) keine identifizierbaren personenbezogenen Daten von Dritten enthalten und (ii) keine identifizierbaren personenbezogenen Daten über Sie enthalten;
 - (c) in jedem Fall für alle anderen durch die Datenschutzgesetze und andere einschlägige Gesetze vorgeschriebenen oder zulässigen Zwecke.
- 3.3. **Ihre Einhaltung der einschlägigen gesetzlichen Bestimmungen und Ihre Anweisungen an Pix4D.** Sie sichern zu und gewährleisten, dass (i) Sie in Bezug auf Ihre Verarbeitung personenbezogener Kundendaten, deren Delegation an Pix4D und alle von Ihnen gegenüber Pix4D erteilten Verarbeitungsanweisungen alle einschlägigen Gesetze einschließlich der Datenschutzgesetze eingehalten haben und auch weiterhin einhalten werden, und dass (ii) Sie alle Hinweise zur Verfügung gestellt und alle Einwilligungen und Rechte eingeholt haben, die im Rahmen der Datenschutzgesetze erforderlich sind, damit Pix4D für die in dieser EULA beschriebenen Zwecke personenbezogene Kundendaten verarbeiten kann, und dass Sie dies auch weiterhin tun werden. Sie allein sind für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Kundendaten und der Mittel, mit denen Sie die personenbezogenen Kundendaten erworben haben, verantwortlich. Unbeschadet der Allgemeingültigkeit des Vorherigen stimmen Sie zu, dass Sie für die Einhaltung aller Gesetze (einschließlich der Datenschutzgesetze), die auf alle über die lizenzierten Angebote im Rahmen der EULA erzeugten, versandten oder verwalteten Inhalte Anwendung finden, verantwortlich sind. Sie ermächtigen und instruieren Pix4D hiermit, Kontolöschungsersuchen von Nutzern selbst in Ihrem Namen zu verwalten und zu bearbeiten, soweit (i) diese Ersuchen vom Nutzer über data_protection@pix4d.com oder auf anderem Wege direkt an Pix4D geschickt

werden und (ii) der Nutzer einer Ihrer autorisierten Nutzer ist. In diesem Fall kann Pix4D Sie von diesem Kontrollöschungsersuchen in Kenntnis setzen, soweit es dies für nötig hält. Die EULA (einschließlich dieser DVV) stellt, zusammen mit der Nutzung und der Weise, in der Sie die lizenzierten Produkte in Übereinstimmung mit der EULA konfiguriert haben, Ihre gesamten Anweisungen an Pix4D in Bezug auf die relevante Verarbeitung der personenbezogenen Kundendaten dar, wobei Sie während der Laufzeit zusätzliche, mit der EULA, der Beschaffenheit, dem Funktionsumfang und der rechtmäßigen Nutzung der lizenzierten Produkte vereinbare Anweisungen übermitteln können, für die Sie, sofern nichts Anderslautendes vereinbart wurde, die anfallenden Kosten tragen. Pix4D hat Sie unverzüglich schriftlich zu informieren, falls es Pix4D zur Kenntnis gelangt oder Pix4D vermutet, dass Anweisungen Ihrerseits bezüglich der Datenverarbeitung gegen europäisches Datenschutzrecht verstoßen.

- 3.4. **Pflichten von Pix4D.** Pix4D hat die personenbezogenen Kundendaten gemäß der EULA in Übereinstimmung mit den einschlägigen Datenschutzgesetzen und Ihren dokumentierten rechtmäßigen Anweisungen wie in Abschnitt 3.2. beschrieben zu verarbeiten.
- 3.5. **Einzelheiten der Verarbeitung.** Gegenstand der Verarbeitung personenbezogener Kundendaten durch Pix4D ist die Erfüllung der EULA. Die Arten personenbezogener Daten und Kategorien betroffener Personen, die Häufigkeit der Übermittlung, die Art der Verarbeitung, der Übermittlungszweck, die Aufbewahrungsfrist und die Einzelheiten der Unterauftragsverarbeitung sind in Anlage C (Beschreibung der Datenübermittlung) zu dieser DVV näher ausgeführt.

4. ERSUCHEN DER BETROFFENEN PERSONEN

Falls Pix4D in Bezug auf personenbezogene Kundendaten während der Laufzeit ein Ersuchen von einer betroffenen Person auf Ausübung ihrer Rechte als betroffene Person gemäß europäischem Datenschutzrecht erhält, wird Pix4D: (i) die betroffene Person anweisen, ihr Ersuchen an Sie zu richten, (ii) Sie umgehend in Kenntnis setzen, und (iii) ohne Ihre vorherige schriftliche Ermächtigung nicht anderweitig auf das Ersuchen der betroffenen Person reagieren, außer wie angemessen (zum Beispiel, um die betroffene Person an Sie zu verweisen) oder rechtlich vorgeschrieben. Darüber hinaus hat Pix4D Ihnen soweit möglich unter Berücksichtigung der Art der Verarbeitung angemessene zusätzliche Unterstützung zu leisten, um Sie in die Lage zu versetzen, Ihren Datenschutzpflichten in Bezug auf die Rechte der betroffenen Person gemäß europäischem Datenschutzrecht nachzukommen. Vorbehaltlich einer vorherigen schriftlichen Vereinbarung zwischen den Parteien verpflichten Sie sich, Pix4D die angemessenen Kosten und Aufwendungen zu erstatten, die Pix4D dabei entstehen, Sie gemäß diesem Abschnitt **¡Error! No se encuentra el origen de la referencia.** zu unterstützen.

5. PIX4D-PERSONAL

Pix4D wird sicherstellen, dass jede Person, die von Pix4D ermächtigt wurde, personenbezogene Kundendaten zu verarbeiten (darunter seine Mitarbeiter, Beauftragten und Auftragnehmer), einer angemessenen (vertraglichen oder gesetzlichen) Verschwiegenheitspflicht unterliegen und sich insbesondere verpflichtet haben, personenbezogene Kundendaten weder an Dritte weiterzugeben noch derartige Daten für andere Zwecke als die Erfüllung ihrer ihnen von Pix4D in Übereinstimmung mit der EULA übertragenen Aufgaben zu nutzen, wobei zwischen den Parteien zudem als vereinbart gilt, dass Pix4D für das Verhalten allen Pix4D-Personals auf dieselbe Weise verantwortlich bleibt wie

für sein eigenes Verhalten.

6. UNTERAUFTRAGSVERARBEITER

- 6.1. **Autorisierte Unterauftragsverarbeiter.** Sie stimmen zu, dass Pix4D Unterauftragsverarbeiter beauftragen darf, um personenbezogene Kundendaten in Ihrem Namen zu verarbeiten. Die derzeit von Pix4D beauftragten und von Ihnen autorisierten Unterauftragsverarbeiter sind (i) Pix4Ds verbundene Unternehmen und (ii) die in Pix4Ds Liste der Unterauftragsverarbeiter, die unter <https://www.pix4d.com/legal> abrufbar ist, genannten Drittparteien. Darüber hinaus erteilen Sie Pix4D hiermit eine schriftliche Ermächtigung, in Übereinstimmung mit diesem Abschnitt beliebige weitere Unterauftragsverarbeiter zu ernennen, um spezifische Verarbeitungstätigkeiten im Namen von Pix4D auszuführen.
- 6.2. **Möglichkeit, Änderungen bei Unterauftragsverarbeitern zu widersprechen.** Soweit europäisches Datenschutzrecht zur Anwendung kommt, wird Pix4D Sie von allen beabsichtigten Änderungen betreffend die Hinzufügung oder Ersetzung seiner Unterauftragsverarbeiter in Kenntnis setzen, und Sie haben dann die Möglichkeit, derartigen Änderungen aus objektiv und sachlich begründbaren Gründen innerhalb von dreißig (30) Tagen nach Inkennntnissetzung zu widersprechen. Falls Sie fristgerecht widersprechen, erhalten Sie Gelegenheit, Ihre Bedenken mit Pix4D zu besprechen, um eine wirtschaftlich angemessene Lösung zu finden. Falls eine derartige Lösung nicht erreicht werden kann, wird Pix4D nach seinem alleinigen Ermessen entweder den neuen Unterauftragsverarbeiter nicht ernennen oder es Ihnen gestatten, die EULA gemäß den Kündigungsbestimmungen der EULA zu kündigen, ohne dass Pix4D dadurch eine Haftung erwächst (aber unbeschadet eventueller Gebühren, die Ihnen vor Kündigung der EULA entstanden sind).
- 6.3. **Anforderungen an die Beauftragung von Unterauftragsverarbeitern.** Pix4D wird bei der Beauftragung von Unterauftragsverarbeitern sicherstellen, dass der Unterauftragsverarbeiter durch Verpflichtungen bezüglich der Verschwiegenheit und des Datenschutzes gebunden ist, die in dem Maß, wie sie auf die Art der Verarbeitungstätigkeiten anwendbar sind, die der Unterauftragsverarbeiter erbringt, mindestens ebenso streng sind wie die Bestimmungen der EULA (einschließlich dieser DVV), wobei als vereinbart gilt, dass Pix4D für das Verhalten aller seiner Unterauftragsverarbeiter ebenso verantwortlich bleibt wie für sein eigenes Verhalten.

7. DATENSICHERHEIT

Pix4D wird angemessene technische und organisatorische Maßnahmen umsetzen und aufrechterhalten, die darauf ausgelegt sind, die personenbezogenen Kundendaten vor versehentlicher oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Weitergabe oder unbefugtem Zugriff zu schützen, darunter insbesondere und mindestens die in Anlage D (Sicherheitsmaßnahmen) dieser DVV (die „**Sicherheitsmaßnahmen**“) festgelegten Maßnahmen. Die Sicherheitsmaßnahmen umfassen Maßnahmen zur Verschlüsselung personenbezogener Kundendaten, um dazu beizutragen, die fortlaufende Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz von Pix4Ds Systemen und Diensten sicherzustellen, dazu beizutragen, den zeitnahen Zugriff auf die personenbezogenen Kundendaten nach einer Verletzung des Schutzes der Daten wiederherzustellen, sowie für regelmäßige Effektivitätstests. Sie sind dafür verantwortlich, die von Pix4D bezüglich der Datensicherheit zur Verfügung gestellten Informationen zu prüfen und eigenständig zu ermitteln, ob die Sicherheitsmaßnahmen Ihre Anforderungen

und rechtlichen Pflichten im Rahmen der Datenschutzgesetze erfüllen. Sie erkennen an, dass die Sicherheitsmaßnahmen dem technischen Fortschritt und der technischen Entwicklung unterliegen und dass Pix4D die Sicherheitsmaßnahmen von Zeit zu Zeit aktualisieren oder modifizieren kann, vorausgesetzt, dass derartige Aktualisierungen und Modifikationen nicht zu einer Verschlechterung der Ihnen zur Verfügung gestellten lizenzierten Angebote führen.

8. DATENÜBERMITTLUNGEN IN NICHT AUF EINER WHITELIST GEFÜHRTE LÄNDER

8.1. **EU SCC.** Die Parteien vereinbaren, dass Pix4D personenbezogene Kundendaten für die Zwecke der Erfüllung der EULA oder in Verbindung mit diesen in nicht auf einer Whitelist geführte Länder übermitteln darf. In Fällen, in denen Pix4D dem europäischen Datenschutzrecht unterliegende personenbezogene Kundendaten (zurück) an Sie als Verantwortlichen, der seinen Sitz in einem nicht auf einer Whitelist geführten Land hat, übermittelt, vereinbaren die Parteien, durch Modul vier (Übermittlung von Auftragsverarbeitern an Verantwortliche) der EU SCC in Anlage A (Modul vier (Übermittlung von Auftragsverarbeitern an Verantwortliche) der EU SCC) und wie folgt zusammengestellt (die „**P-C-Klauseln**“), einschließlich aller einschlägigen länderspezifischen Ergänzungen in Anlage B (Länderspezifische Ergänzungen zu den EU SCC) zu dieser DVV, gebunden zu sein und dieses einzuhalten, wobei Pix4D der „Datenexporteur“ ist und Sie der „Datenimporteur“ sind:

- (d) Klauseln 1-6;
- (e) Klausel 7 findet keine Anwendung;
- (f) Klausel 8 mit den Bestimmungen für „Modul vier“, einschließlich des einleitenden Absatzes;
- (g) Klausel 10 mit den Bestimmungen für „Modul vier“;
- (h) Klausel 11 a), aber ohne die Bestimmungen der „Option“ aus Klausel 11 a);
- (i) Klausel 12 mit den Bestimmungen für „Modul vier“; soweit dies nicht im Widerspruch zu den EU SCC steht, wird die Haftung zwischen dem Datenimporteur und dem Datenexporteur (aber nicht gegenüber den betroffenen Personen) begrenzt/ausgeschlossen wie in Abschnitt 14 dieser DVV festgelegt;
- (j) Klauseln 14-15 mit den Bestimmungen für „Modul vier“, insoweit wie der Datenexporteur vom Datenimporteur erhaltene Daten mit vom Datenexporteur in einem auf einer Whitelist geführten Land erfassten personenbezogenen Daten zusammenführt;
- (k) Klausel 16 mit den Bestimmungen für „Modul vier“;
- (l) Klausel 17 mit den Bestimmungen für „Modul vier“, wobei das Recht Frankreichs das von den Parteien für die Zwecke von Klausel 17 vereinbarte Recht ist;
- (m) Klausel 18 mit den Bestimmungen für „Modul vier“, wobei die Gerichte von Frankreich das von den Parteien für die Zwecke von Klausel 18 vereinbarte Recht sind.

8.2. **Anhänge zu den EU SCC.** Die Anhänge, auf die durch die P-C-Klauseln verwiesen wird, werden wie folgt gebildet:

- (a) Anhang I.A besteht aus:
 - i. den in der EULA festgelegten und von Ihnen in dem betreffenden

Organisationsformular übermittelten Informationen, wobei Pix4D der als „Auftragsverarbeiter“ handelnde „Datenexporteur“ ist und Sie der als „Verantwortlicher“ handelnde „Datenimporteur“ sind;

- ii. den Kontaktdaten des Datenexporteurs: Die Kontaktdaten für den Datenexporteur sind: Pix4D SA, Route de Renens 24, 1008 Prilly, Schweiz. Das Datenschutzteam des Datenexporteurs kann unter der folgenden E-Mail-Adresse kontaktiert werden: data_protection@pix4d.com. Der Datenschutzbeauftragte des Datenexporteurs kann wie folgt kontaktiert werden: Parrot Drones, c/o Victor Vuillard, 174 Quai de Jemmapes, 75010 Paris, Frankreich;
 - iii. den Kontaktdaten des Datenimporteurs: Die Kontaktdaten für den Datenimporteur, einschließlich der Kontaktdaten seines Datenschutzbeauftragten, stehen dem Datenexporteur in dem betreffenden Organisationsformular zur Verfügung (sofern diese Daten vom Datenimporteur zur Verfügung gestellt wurden) und/oder können vom Datenexporteur in Einzelfällen später angefordert werden;
 - iv. den in Anlage C (*Beschreibung der Datenübermittlung*) dieser DVV beschriebenen Tätigkeiten;
 - v. die Parteien vereinbaren, dass die Ausfertigung der EULA durch Datenimporteur und Datenexporteur die Ausfertigung dieser P-C-Klauseln durch beide Parteien per Wirksamkeitsdatum der Bedingungen darstellt.
- (b) Anhang I.B besteht aus dem relevanten Abschnitt der Anlage C (*Beschreibung der Datenübermittlung*);
- (c) Anhang II besteht aus Anlage B (*Technische und organisatorische Maßnahmen*) dieser DVV.
- (d) Anhang III, sofern anwendbar, besteht aus Pix4Ds Liste der Unterauftragsverarbeiter, die unter <https://www.pix4d.com/legal> abrufbar ist.

8.3. **Beurteilung der Auswirkungen der Datenübermittlung.** Der Kunde bestätigt, dass die geplanten Übermittlungen personenbezogener Daten durch Pix4D (zurück) an den Kunden nach seinem besten Wissen gemäß einschlägigem Recht zulässig sind, und die Parteien haben keinen Grund zu der Annahme, dass die beabsichtigten Datenübermittlungen unbefugt sind.

8.4. **Schadloshaltung.** Jede Partei hat die andere Partei im Falle von Ansprüchen Dritter aufgrund einer Verletzung ihrer Pflichten aus den P-C-Klauseln zu entschädigen.

9. VERLETZUNGEN DES SCHUTZES DER DATEN

Falls Pix4D eine Verletzung des Schutzes von Daten zur Kenntnis gelangt, hat Pix4D: (i) Sie ohne unangemessene Verzögerung und, soweit machbar, keinesfalls später als achtundvierzig (48) Stunden, nachdem es von der Verletzung des Schutzes der Daten erfährt, davon in Kenntnis zu setzen, (ii) zeitnahe Angaben bezüglich der Verletzung des Schutzes der Daten zur Verfügung zu stellen, wenn diese bekannt werden oder so wie von Ihnen begründetermaßen angefordert, und (iii) unverzüglich angemessene Schritte zu unternehmen, um jede Verletzung des Schutzes der Daten einzudämmen und zu untersuchen. Pix4Ds Mitteilung über eine Verletzung des Schutzes der Daten, bzw. seine Reaktion darauf, gemäß diesem Abschnitt ist nicht als Schuld- oder Haftungsanerkennnis durch Pix4D in Bezug auf die Verletzung des Schutzes der Daten auszulegen.

10. STAATLICHE ERSUCHEN UM AUSKUNFT ÜBER DATEN

Pix4D gewährt, wenn es als Ihr Auftragsverarbeiter gemäß europäischem Datenschutzrecht personenbezogene Kundendaten verarbeitet, staatlichen Einrichtungen oder Behörden einschließlich von Strafverfolgungsbehörden keinen Zugriff auf Informationen über Pix4D-Konten einschließlich von Kundendaten, sofern es nicht durch einschlägiges Recht dazu verpflichtet ist. Die mit einer Reaktion auf ein verpflichtendes Ersuchen (sei es durch eine Vorladung, einen Gerichtsbeschluss, einen Durchsuchungsbeschluss oder ein sonstiges gültiges rechtliches Verfahren) seitens einer staatlichen Einrichtung oder Behörde einschließlich von Strafverfolgungsbehörden um Zugriff oder Auskunft über ein Pix4D-Konto, einschließlich von Ihnen und/oder den autorisierten Nutzern gehörenden Kundendaten, verbundenen Kosten sind von Ihnen zu tragen.

11. ÜBERPRÜFUNG UND AUDIT DER EINHALTUNG VON BESTIMMUNGEN

Pix4D hat Ihnen alle Informationen zur Verfügung zu stellen, die begründetermaßen erforderlich sind, um die Einhaltung seiner Pflichten aus dieser DVV nachzuweisen, und hat Audits einschließlich von Ermittlungen, die von Ihnen oder einem von Ihnen ernannten unabhängigen Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen, um Pix4Ds Einhaltung seiner Pflichten aus dieser DVV zu verifizieren, vorbehaltlich üblicher Verschwiegenheitszusagen. Darüber hinaus kann Ihnen Pix4D kostenlos unaufgefordert oder auf Ihr Ersuchen hin alle von Pix4Ds Auditor erstellten Auditberichte zur Verfügung stellen, die Pix4Ds Einhaltung dieser DVV bestätigen.

12. BEURTEILUNGEN DER AUSWIRKUNGEN UND KONSULTATIONEN

Soweit gemäß den einschlägigen Datenschutzgesetzen erforderlich, hat Pix4D, unter Berücksichtigung der Art der Verarbeitung und der Pix4D zur Verfügung stehenden Informationen, alle begründetermaßen angeforderten Informationen bezüglich der lizenzierten Angebote zur Verfügung zu stellen, um es Ihnen zu ermöglichen, Beurteilungen der Auswirkungen auf den Datenschutz oder vorherige Konsultationen mit Datenschutzbehörden so wie durch die Datenschutzgesetze vorgeschrieben durchzuführen. In Abhängigkeit von einer vorherigen schriftlichen Vereinbarung zwischen den Parteien werden Sie Pix4D die angemessenen Kosten und Aufwendungen erstatten, die Pix4D dabei entstehen, Sie gemäß diesem Abschnitt **¡Error! No se encuentra el origen de la referencia.** zu unterstützen.

13. RÜCKGABE ODER LÖSCHUNG VON DATEN

Mit Kündigung oder Ablauf der EULA hat Pix4D (auf Ihre Wahl hin) alle personenbezogenen Kundendaten (einschließlich von Kopien) in seinem Besitz oder unter seiner Kontrolle zu löschen (einschließlich per Anonymisierung) oder sie Ihnen zurückzugeben, mit der Ausnahme, dass diese Anforderung insoweit keine Anwendung findet, wie Pix4D durch einschlägiges Recht verpflichtet ist, einige oder alle der personenbezogenen Kundendaten oder personenbezogene Kundendaten, die es auf Backup-Systemen gespeichert hat, aufzubewahren, wobei Pix4D diese personenbezogenen Kundendaten sicher von anderen Daten zu trennen, sie vor weiterer Verarbeitung zu schützen und letztlich in Übereinstimmung mit Pix4Ds Lösungsrichtlinien zu löschen hat, außer wie durch einschlägiges Recht vorgeschrieben.

14. HAFTUNGSBESCHRÄNKUNG

Außer soweit gemäß den in den Abschnitten 8.1 und 8.2 enthaltenen P-C-Klauseln festgelegt und außer soweit in dieser DVV ausdrücklich vereinbart, werden Pix4Ds Haftung bzw. Ihre Haftung soweit gemäß einschlägigem Recht zulässig ausgeschlossen.

15. VERSCHIEDENES

- 15.1. **Ergänzungen.** Jede Ergänzung an dieser DVV hat schriftlich zu erfolgen und ist durch den entsprechend befugten Vertreter der Parteien ordnungsgemäß zu unterzeichnen.
- 15.2. **Widersprüche.** Im Falle eines Widerspruchs oder einer Unvereinbarkeit zwischen dieser DVV und der EULA, der/die die Verarbeitung der personenbezogenen Kundendaten betrifft, sind die Bestimmungen der folgenden Dokumente (in dieser Reihenfolge) maßgeblich: (i) EU SCC, dann (ii) diese DVV, und dann (iii) die EULA.
- 15.3. **Salvatorische Klausel.** Falls eine Bestimmung der DVV aus beliebigem Grund für nicht durchsetzbar befunden wird, ist sie, falls möglich, anzupassen statt für nichtig zu erklären, um der rechtlichen und wirtschaftlichen Absicht der Parteien möglichst nahezukommen. In jedem Fall bleiben alle sonstigen Bestimmungen der DVV im vollsten möglichen Umfang gültig und durchsetzbar.
- 15.4. **Mitteilungen.** Für die Zwecke sämtlicher Schriftwechsel zwischen den Parteien gilt, dass jede in Verbindung mit der EULA getätigte Benachrichtigung oder sonstige Mitteilung der Schriftform bedarf (wobei die elektronische Form als ausreichend gilt) und per E-Mail an die folgenden Adressen zu senden ist:

Falls an Pix4D: E-Mail: legal@pix4d.com.

Falls an Sie: an die in Ihrem Konto hinterlegte E-M-Adresse. Im Falle einer Änderung liegt es in Ihrer alleinigen Verantwortung, Pix4D von Ihren neuen Kontaktdaten in Kenntnis zu setzen. Zu diesem Zweck können Sie entweder Pix4Ds Supportteam unter <https://support.pix4d.com> kontaktieren oder Ihre Kontaktdaten in Ihrem Konto aktualisieren.

Wenn und falls genutzt, dient das von Pix4D genutzte elektronische Kommunikationssystem als alleiniger Nachweis für den Inhalt und Zeitpunkt der Zustellung und des Erhalts dieser elektronischen Mitteilungen.

- 15.5. **Kosten.** Jede Partei hat in Verbindung mit der Einhaltung dieser DVV, einschließlich der P-C-Klauseln wie jeweils anwendbar, ihre eigenen Kosten zu tragen.

16. ANWENDBARES RECHT – BEILEGUNG VON STREITIGKEITEN

- 16.1. **Anwendbares Recht.** Unabhängig vom anwendbaren Recht der EULA unterliegt diese DVV ausschließlich dem materiellen Recht der Schweiz und ist gemäß diesem auszulegen, wobei (i) internationale Übereinkommen, einschließlich des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11.04.1980 (CISG), und (ii) die Schweizer Kollisionsnormen auf diese DVV ausdrücklich keine Anwendung finden.
- 16.2. **Zuständigkeit und Gerichtsstand.** Unabhängig vom Gerichtsstand der EULA haben die ordentlichen Gerichte von Lausanne, Schweiz, die ausschließliche

Zuständigkeit in Bezug auf alle zwischen den Parteien aus dieser DVV herrührenden oder damit in Verbindung stehenden Streitigkeiten.

17. ZUSÄTZLICHE BESTIMMUNGEN FÜR KALIFORNISCHE PERSONENBEZOGENE INFORMATIONEN

- 17.1. **Geltungsbereich und Anwendbarkeit.** Dieser Abschnitt **¡Error! No se encuentra el origen de la referencia.** der DVV gilt zusätzlich zu den Bestimmungen dieser DVV insoweit, wie Pix4D im Rahmen der EULA kalifornische personenbezogene Informationen gemäß CCPA verarbeitet. Im Falle eines Widerspruchs oder einer Mehrdeutigkeit zwischen diesem Abschnitt **¡Error! No se encuentra el origen de la referencia.** und allen sonstigen Bestimmungen dieser DVV ist dieser Abschnitt **¡Error! No se encuentra el origen de la referencia.** maßgeblich, aber nur soweit dieser Abschnitt auf Pix4D anwendbar ist.
- 17.2. **Rollen der Parteien.** Bezüglich der Verarbeitung kalifornischer personenbezogener Informationen gemäß Ihren Anweisungen erkennen die Parteien an und vereinbaren, dass Sie für die Zwecke des CCPA ein Unternehmen sind und Pix4D ein Dienstleister.
- 17.3. **Verantwortlichkeiten.** Die Parteien vereinbaren, dass Pix4D kalifornische personenbezogene Informationen als Dienstleister streng für den Zweck der Lizenzierung der lizenzierten Angebote im Rahmen der EULA (der „**Geschäftszweck**“) oder wie anderweitig durch den CCPA gestattet verarbeiten wird.

18. DEFINITIONEN

Zusatzbedingungen	hat die ihm auf der ersten Seite zugewiesene Bedeutung.
Autorisierte Nutzer	bezeichnet die Personen, denen die Nutzung der lizenzierten Produkte von Ihnen in Übereinstimmung mit der EULA gestattet wurde. Um der Klarheit willen wird festgestellt, dass der Begriff „autorisierte Nutzer“ Ihre Beschäftigten, verbundenen Unternehmen und sonstige Drittparteien außerhalb Ihrer Einrichtung umfassen kann, die von Ihrem Kontoadministrator ordnungsgemäß ermächtigt wurden, Mitglieder einer Organisation zu werden, in der Sie als Verantwortlicher dieser Drittparteien handeln.
Unternehmen (Business)	hat die ihm im CCPA gegebene Bedeutung.
Geschäftszweck	hat die ihm in Abschnitt 17.3. zugewiesene Bedeutung.
Kalifornische personenbezogene Informationen	bezeichnet personenbezogene Daten, die dem Schutz des CCPA unterliegen.
CCPA	Bezeichnet den California Civil Code Sec. 1798.100 et seq., auch bekannt als California Consumer Privacy Act von 2018.
CNIL	bezeichnet die Commission Nationale de l'Informatique et

des Libertés im Einklang mit der Bedeutung in Abschnitt 8.2.

Verbraucher (Consumer)	hat die ihm im CCPA gegebene Bedeutung.
Verantwortlicher	bezeichnet die natürliche oder juristische Person, staatliche Einrichtung, Behörde oder sonstige Organisation, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.
Kundendaten	bezeichnet die von Ihnen oder Endnutzern oder im Namen von Ihnen oder Endnutzern mittels der lizenzierten Angebote und im Rahmen des Kontos zur Verfügung gestellten Daten.
Personenbezogene Kundendaten	bezeichnet die in den Kundendaten enthaltenen personenbezogenen Daten, einschließlich eventueller Sonderkategorien personenbezogener Daten.
Verletzung des Schutzes der Daten	bezeichnet eine Sicherheitsverletzung, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu durch Pix4D übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten führt, insbesondere einen Verstoß gegen <u>Anlage D (Sicherheitsmaßnahmen)</u> .
Datenschutzgesetze	bezeichnet alle Datenschutzgesetze und -verordnungen, die auf Pix4Ds oder Ihre Verarbeitung personenbezogener Kundendaten im Rahmen der EULA anwendbar sind, einschließlich, je nach Sachlage, des europäischen und außereuropäischen Datenschutzrechts.
Betroffene Person	bezeichnet jede identifizierte oder identifizierbare natürliche Person, auf die sich personenbezogene Daten beziehen.
Ersuchen der betroffenen Person	hat die ihm in Abschnitt ¡Error! No se encuentra el origen de la referencia. zugewiesene Bedeutung.
DVV	hat die ihm auf der ersten Seite zugewiesene Bedeutung.
EWR	bezeichnet den Europäischen Wirtschaftsraum.
EULA	hat die ihm auf der ersten Seite zugewiesene Bedeutung.
EU SCC	bezeichnet die Standardvertragsklauseln, so wie sie durch die Entscheidung der Europäischen Kommission vom 4. Juni 2021 [C(2021)3972 final] zu Standardvertragsklauseln zur Übermittlung von personenbezogenen Daten in Drittländer gemäß Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates genehmigt

wurden, und alle Änderungen daran.

**Europäisches
Datenschutzrecht**

bezeichnet, je nach Sachlage, (a) die DSGVO und eventuelle lokale, Landes- und Bundesgesetze, die die DSGVO umsetzen, (b) die GDPR des Vereinigten Königreichs und (c) das schweizerische DSG und, in jedem Fall, jegliche neue oder überarbeitete Fassung derselben, die während der Laufzeit in Kraft tritt.

EDÖB

bezeichnet den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) in der in Abschnitt 8.2 enthaltenen Bedeutung.

DSGVO

bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), und jede neue oder überarbeitete Fassung derselben, die während der Laufzeit in Kraft tritt.

**Allgemeine
Bedingungen**

hat die ihm auf der ersten Seite zugewiesene Bedeutung.

**Außereuropäisches
Datenschutzrecht**

bezeichnet die außerhalb des EWR, des Vereinigten Königreichs und der Schweiz in Kraft befindlichen Datenschutzgesetze, insbesondere den CCPA.

Organisationsformular

bezeichnet die Organisationseinstellungen innerhalb des EUM, das von Pix4D zur Anmeldung Ihres Kontos zur Verfügung gestellt wird.

Parteien

hat die ihm auf der ersten Seite zugewiesene Bedeutung.

P-C-Klauseln

bezeichnet Modul vier (Übermittlung von Auftragsverarbeitern an Verantwortliche) der EU SCC wie in den Abschnitten 8.1 und 8.2 dieser DVV zusammengestellt und dargelegt.

Pix4D, uns, unser

bezeichnen Pix4D SA, eine Schweizer Aktiengesellschaft (*société anonyme*), eingetragen in der Schweiz unter der Nummer CHE-207.009.701, mit eingetragenem Geschäftssitz in der Route de Renens 24, 1008 Prilly, Schweiz.

**Sicherheits-
maßnahmen**

bezeichnet die in Anlage D (*Sicherheitsmaßnahmen*) beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen.

**Dienstleister (Service
Provider)**

hat die ihm im CCPA gegebene Bedeutung.

Schweizerisches DSG

bezeichnet das schweizerische Bundesgesetz über den Datenschutz vom 19. Juni 1992 und die schweizerische

Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 und, in jedem Fall, jede neue oder überarbeitete Fassung derselben, die während der Laufzeit in Kraft tritt.

Laufzeit	bezeichnet den Zeitraum vom Wirksamkeitsdatum der Bedingungen bis zum Ende von Pix4Ds Bereitstellung der lizenzierten Angebote, einschließlich, sofern anwendbar, jedes Zeitraums, in dem die Bereitstellung der lizenzierten Angebote ausgesetzt ist, und jedes Zeitraums nach einer Kündigung, in dem Pix4D die lizenzierten Angebote zu Übergangszwecken weiter bereitstellt.
Wirksamkeitsdatum der Bedingungen	bezeichnet das Datum, an dem Sie diese DVV akzeptiert oder die Parteien sie anderweitig vereinbart haben.
GDPR des Vereinigten Königreichs	bezeichnet die DSGVO der EU in ihrer ergänzten und gemäß dem European Union (Withdrawal) Act 2018 des Vereinigten Königreichs in das Recht des Vereinigten Königreichs überführten Fassung und die einschlägige Sekundärgesetzgebung im Rahmen dieses Gesetzes, sowie jede neue oder überarbeitete Fassung derselben, die während der Laufzeit in Kraft tritt.
Auf einer Whitelist geführte Länder	bezeichnet: - <i>für der DSGVO unterliegende personenbezogene Kundendaten:</i> den EWR oder ein Land oder Territorium, das Gegenstand eines Angemessenheitsbeschlusses durch die Europäische Kommission gemäß Artikel 45(1) der DSGVO ist; - <i>für der GDPR des Vereinigten Königreichs unterliegende personenbezogene Kundendaten:</i> das Vereinigte Königreich oder ein Land oder Territorium, das Gegenstand der Angemessenheitsregeln gemäß Artikel 45(1) der britischen GDPR und Abschnitt 17A des Data Protection Act 2018 ist; und/oder - <i>für dem schweizerischen DSG unterliegende personenbezogene Kundendaten:</i> die Schweiz oder ein Land oder Territorium, das (i) in der vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten veröffentlichten Liste der Staaten enthalten ist, deren Gesetzgebung ein angemessenes Maß an Schutz bietet, oder, je nach Sachlage, (ii) Gegenstand eines Angemessenheitsbeschlusses durch den Schweizerischen Bundesrat gemäß dem schweizerischen DSG ist.
Sie und Ihr	bezeichnet die juristische Person, die die lizenzierten Angebote im Rahmen der EULA zur Nutzung durch ihre autorisierten Nutzer lizenziert.

Die Begriffe „personenbezogene Daten“, „betroffene Person“, „verarbeiten“, „Verantwortlicher“ und „Auftragsverarbeiter“ so wie in dieser DVV verwendet haben die ihnen in der DSGVO gegebenen Bedeutungen, unabhängig davon, ob europäisches Datenschutzrecht oder außereuropäisches Datenschutzrecht Anwendung findet.

Anlagen:

Anlage A: Modul vier (Übermittlung von Auftragsverarbeitern an Verantwortliche) der EU SCC

Anlage B: Länderspezifische Ergänzungen zu den EU SCC

Anlage C: Beschreibung der Datenübermittlung

Anlage D: Sicherheitsmaßnahmen

Anlage A: Modul vier (Übermittlung von Auftragsverarbeitern an Verantwortliche) der EU SCC

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

- a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ⁽¹⁾ bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.
- b) Die Parteien:
- i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und
 - ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“),
- haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) einverstanden erklärt.
- c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.
- d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

- a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder

¹ Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

- b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3 Drittbegünstigte

- a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:
 - i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7
 - ii) Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b
 - iii) N/A
 - iv) N/A
 - v) Klausel 13
 - vi) Klausel 15.1 Buchstaben c, d und e
 - vii) Klausel 16 Buchstabe e
 - viii) Klausel 18
- b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe a unberührt.

Klausel 4 Auslegung

- a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.
- b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.
- c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6 Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang I.B aufgeführt.

Klausel 7 – fakultativ Kopplungsklausel

- a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als

Datenimporteur beitreten, indem sie die Anlage ausfüllt und Anhang I.A unterzeichnet.

- b) Nach Ausfüllen der Anlage und Unterzeichnung von Anhang I.A wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in Anhang I.A.
- c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8 ***Datenschutzgarantien***

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

8.1 Weisungen

- a) Der Datenexporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenimporteurs, der als sein Verantwortlicher fungiert.
- b) Der Datenexporteur unterrichtet den Datenimporteur unverzüglich, wenn er die betreffenden Weisungen nicht befolgen kann, u. a. wenn eine solche Weisung gegen die Verordnung (EU) 2016/679 oder andere Datenschutzvorschriften der Union oder eines Mitgliedstaats verstößt.
- c) Der Datenimporteur sieht von jeglicher Handlung ab, die den Datenexporteur an der Erfüllung seiner Pflichten gemäß der Verordnung (EU) 2016/679 hindern würde, einschließlich im Zusammenhang mit Unterverarbeitungen oder der Zusammenarbeit mit den zuständigen Aufsichtsbehörden.
- d) Nach Wahl des Datenimporteurs löscht der Datenexporteur nach Beendigung der Datenverarbeitungsdienste alle im Auftrag des Datenimporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenimporteur, dass dies erfolgt ist, oder gibt dem Datenimporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien.

8.2 Sicherheit der Verarbeitung

- a) Die Parteien treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten, auch während der Übermittlung, sowie den Schutz vor einer Verletzung der Sicherheit zu gewährleisten, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art der personenbezogenen Daten ⁽²⁾, der Art, dem

² Hierzu zählt, ob die Übermittlung und Weiterverarbeitung personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die

Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung und ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Übermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

- b) Der Datenexporteur unterstützt den Datenimporteur bei der Gewährleistung einer angemessenen Sicherheit der Daten gemäß Buchstabe a. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Datenexporteur gemäß diesen Klauseln verarbeiteten personenbezogenen Daten meldet der Datenexporteur dem Datenimporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde, und unterstützt den Datenimporteur bei der Behebung der Verletzung.
- c) Der Datenexporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.3 Dokumentation und Einhaltung der Klauseln

- a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
- b) Der Datenexporteur stellt dem Datenimporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung seiner Pflichten gemäß diesen Klauseln erforderlich sind, und ermöglicht Prüfungen und trägt zu diesen bei.

Klausel 9

Einsatz von Unterauftragsverarbeitern

N/A

Klausel 10

Rechte betroffener Personen

Die Parteien unterstützen sich gegenseitig bei der Beantwortung von Anfragen und Anträgen, die von betroffenen Personen gemäß den für den Datenimporteur geltenden lokalen Rechtsvorschriften oder — bei der Datenverarbeitung durch den Datenexporteur in der Union — gemäß der Verordnung (EU) 2016/679 gestellt werden.

Klausel 11

Rechtsbehelf

- a) Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

[OPTION: Der Datenimporteur erklärt sich damit einverstanden, dass betroffene Personen eine Beschwerde auch bei einer unabhängigen Streitbeilegungsstelle

Gewerkschaftszugehörigkeit hervorgehen, oder genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten enthalten.

(³)einreichen können, ohne dass für die betroffene Person Kosten entstehen. Er unterrichtet die betroffenen Personen in der unter Buchstabe a beschriebenen Weise über einen solchen Rechtsbehelfsmechanismus sowie darüber, dass sie nicht verpflichtet sind, davon Gebrauch zu machen oder bei der Einlegung eines Rechtsbehelfs eine bestimmte Reihenfolge einzuhalten.]

Klausel 12 **Haftung**

- a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.
- b) Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.
- c) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.
- d) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe c haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.
- e) Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

Klausel 13 **Aufsicht**

N/A

ABSCHNITT III — LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

(wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden)

- a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten,

³ Der Datenimporteur darf eine unabhängige Streitbeilegung über eine Schiedsstelle nur dann anbieten, wenn er in einem Land niedergelassen ist, das das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche ratifiziert hat.

den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

- b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:
 - i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,
 - ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien, ⁽⁴⁾
 - iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.
- c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.
- d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe b zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe a im Einklang stehen; hierunter fällt auch eine Änderung der

⁴ Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. Dies betrifft insbesondere interne Aufzeichnungen oder sonstige Belege, die fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden, sofern diese Informationen rechtmäßig an Dritte weitergegeben werden können. Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden; den Parteien obliegt die sorgfältige Prüfung, ob alle diese Elemente ausreichend zuverlässig und repräsentativ sind, um die getroffene Schlussfolgerung zu bekräftigen. Insbesondere müssen die Parteien berücksichtigen, ob ihre praktische Erfahrung durch öffentlich verfügbare oder anderweitig zugängliche zuverlässige Informationen über das Vorhandensein oder Nicht-Vorhandensein von Ersuchen innerhalb desselben Wirtschaftszweigs und/oder über die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsgremien, erhärtet und nicht widerlegt wird.

Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe a im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.

- f) Nach einer Benachrichtigung gemäß Buchstabe e oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben d und e Anwendung.

Klausel 15

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

(wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden)

15.1 Benachrichtigung

- a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,
- i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder
 - ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.
- b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden

können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

- c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).
- d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben a bis c während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- e) Die Buchstaben a bis c gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe e und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2 Überprüfung der Rechtmäßigkeit und Datenminimierung

- a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14 Buchstabe e.
- b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.
- c) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV — SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

- a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
- b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe f.
- c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
 - i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe b ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,
 - ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder
 - iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

- d) Von dem in der EU ansässigen Datenexporteur erhobene personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen unverzüglich vollständig gelöscht werden, einschließlich aller Kopien. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.
- e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz 3 der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17
Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines Landes, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von _____ (*Land angeben*) ist.

Klausel 18
Gerichtsstand und Zuständigkeit

Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten von _____ (*Land angeben*) beigelegt.

ANLAGE

ERLÄUTERUNG:

Es muss möglich sein, die für jede Datenübermittlung oder jede Kategorie von Datenübermittlungen geltenden Informationen klar voneinander zu unterscheiden und in diesem Zusammenhang die jeweilige(n) Rolle(n) der Parteien als Datenexporteur(e) und/oder Datenimporteur(e) zu bestimmen. Dies erfordert nicht zwingend, dass für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen und/oder für jedes Vertragsverhältnis getrennte Anlagen ausgefüllt und unterzeichnet werden müssen, sofern die geforderte Transparenz bei Verwendung einer einzigen Anlage erzielt werden kann. Erforderlichenfalls sollten getrennte Anlagen verwendet werden, um ausreichende Klarheit zu gewährleisten.

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur(e): *[Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihrer Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union]*

1.

Name: _____

Anschrift: _____

Name, Funktion und Kontaktdaten der Kontaktperson: _____

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: _____

Unterschrift und Datum: _____

Rolle (Verantwortlicher/Auftragsverarbeiter): _____

2.

Datenimporteur(e): *[Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson]*

1.

Name: _____

Anschrift: _____

Name, Funktion und Kontaktdaten der Kontaktperson: _____

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: _____

Unterschrift und Datum: _____

Rolle (Verantwortlicher/Auftragsverarbeiter): _____

2.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

Kategorien der übermittelten personenbezogenen Daten

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden)

Art der Verarbeitung

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

Anlage B: Länderspezifische Ergänzungen zu den EU SCC

Schweiz

Für die Zwecke des schweizerischen DSG gilt, dass, wo Übermittlungen personenbezogener Kundendaten im Rahmen der EULA der DSGVO und dem schweizerischen DSG unterliegen, die P-C-Klauseln wie laut Abschnitten 8.1 und 8.2 dieser DPA anwendbar mit den folgenden Änderungen gelten (um Zweifel auszuschließen wird festgestellt, dass diese Änderungen die P-C-Klauseln wie für die Zwecke der DSGVO anwendbar unberührt lassen):

- Verweise auf „Verordnung (EU) 2016/679“ oder auf „diese Verordnung“ sind, soweit anwendbar, als Verweise auf das schweizerische DSG auszulegen.
- Verweise auf „Verordnung (EU) 2018/1725“ werden gestrichen.
- Verweise auf „Union“, „EU“ und „EU-Mitgliedstaat“ sind so auszulegen, als bezeichneten sie die Schweiz.
- Klausel 17 wird durch folgenden Text ersetzt: „Diese Klauseln unterliegen den Gesetzen der Schweiz, soweit die Übermittlungen dem schweizerischen DSG unterliegen.“
- Klausel 18 wird durch folgenden Text ersetzt:
„Jeder Streit, der sich aus diesen Klauseln ergibt und sich auf das schweizerische DSG bezieht, ist durch die Gerichte der Schweiz beizulegen. Eine betroffene Person kann zudem Klage gegen den Datenexporteur und/oder Datenimporteur bei den Gerichten der Schweiz einreichen, in deren Zuständigkeitsbereich sie ihren gewöhnlichen Aufenthaltsort hat. Die Parteien vereinbaren, sich der Zuständigkeit dieser Gerichte zu unterwerfen.“
- Bis zum Inkrafttreten des überarbeiteten schweizerischen DSG schützen die P-C-Klauseln auch personenbezogene Daten juristischer Personen, und juristische Personen erhalten im Rahmen der P-C-Klauseln denselben Schutz wie natürliche Personen.

Für die Zwecke des schweizerischen DSG finden dort, wo Übermittlungen personenbezogener Kundendaten im Rahmen der EULA ausschließlich dem schweizerischen DSG unterliegen, die laut den Abschnitten 8.1 und 8.2 dieser DVV anzuwendenden P-C-Klauseln mit den folgenden Änderungen Anwendung:

- Verweise auf „Verordnung (EU) 2016/679“ oder auf „diese Verordnung“ sind als Verweise auf das schweizerische DSG auszulegen.
- Verweise auf „Verordnung (EU) 2018/1725“ werden gestrichen.
- Verweise auf „Union“, „EU“ und „EU-Mitgliedstaat“ sind so auszulegen, als bezeichneten sie die Schweiz.
- Klausel 17 wird durch folgenden Text ersetzt: „Diese Klauseln unterliegen den Gesetzen der Schweiz.“
- Klausel 18 wird durch folgenden Text ersetzt:

„Jeder Streit, der sich aus diesen Klauseln ergibt und sich auf das schweizerische DSG bezieht, ist durch die Gerichte der Schweiz beizulegen. Eine betroffene Person kann zudem Klage gegen den Datenexporteur und/oder Datenimporteur bei den Gerichten der Schweiz einreichen, in deren Zuständigkeitsbereich sie ihren gewöhnlichen Aufenthaltsort hat. Die Parteien vereinbaren, sich der Zuständigkeit dieser Gerichte zu unterwerfen.“

- Bis zum Inkrafttreten des überarbeiteten schweizerischen DSG schützen die P-C-Klauseln auch personenbezogene Daten juristischer Personen, und juristische Personen erhalten im Rahmen der P-C-Klauseln denselben Schutz wie natürliche Personen.

Anlage C: Beschreibung der Datenübermittlung

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden:

Betroffene Personen umfassen Personen, über die Pix4D von Ihnen (oder auf Ihre Anweisung hin) oder von autorisierten Nutzern, einschließlich von in den Inhalten erscheinenden Drittparteien, mittels der lizenzierten Angebote Daten zur Verfügung gestellt werden.

Kategorien der übermittelten personenbezogenen Daten:

Daten in Bezug auf Personen, die Pix4D von Ihnen (oder auf Ihre Anweisung hin) oder von autorisierten Nutzern mittels der Dienste zur Verfügung gestellt werden, einschließlich von personenbezogenen Daten in den Inhalten erscheinender Drittparteien.

Übermittelte sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

Die Parteien gehen nicht von der Übermittlung sensibler Daten aus.

Häufigkeit der Übermittlung (z. B. ob die Daten einmalig oder kontinuierlich übermittelt werden):

Regelmäßig und fortlaufend

Art der Verarbeitung:

Pix4D wird personenbezogene Kundendaten für die Zwecke verarbeiten, die lizenzierten Angebote zur Nutzung durch Sie und die autorisierten Nutzer in Übereinstimmung mit der EULA zur Verfügung zu stellen.

Zweck(e) der Datenübermittlung und Weiterverarbeitung:

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer:

Die Laufzeit zuzüglich des Zeitraums vom Ende der Laufzeit bis zur Löschung sämtlicher Kundendaten durch Pix4D in Übereinstimmung mit der EULA und dieser DVV.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben:

Siehe Pix4Ds Liste der Unterauftragsverarbeiter, die unter <https://www.pix4d.com/legal> abgerufen werden kann

Anlage D: Sicherheitsmaßnahmen

Der folgende Text enthält die Beschreibung der technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen), die Pix4D umgesetzt hat, um ein angemessenes Sicherheitsniveau sicherzustellen (die „**Sicherheitsmaßnahmen**“), das die Art, den Umfang, den Kontext und den Verarbeitungszweck sowie die Risiken für die und die Freiheiten der betroffenen Personen berücksichtigt:

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten
 - a) Die Pseudonymisierung wird so durchgeführt, dass Daten ohne zusätzliche Informationen nicht einer bestimmten betroffenen Person zugeordnet werden können.
 - b) Zusätzliche Informationen für die Zuordnung personenbezogener Daten zu einer bestimmten betroffenen Person werden in gesonderten und sicheren Systemen aufbewahrt, die nur einer begrenzten Anzahl von Personen zugänglich sind.
 - c) Bei der Verschlüsselung personenbezogener Daten werden Algorithmen und Schlüssellänge im Verhältnis zum Grad der Sensibilität der Daten gehalten.
 - d) Die Verschlüsselungsschlüssel werden sicher aufbewahrt und nur einer begrenzten Zahl von Personen gegeben.
 - e) Interne Anweisungen stellen sicher, dass im Falle einer Offenlegung oder selbst nach Ablauf der gesetzlichen Löschungsfrist soweit möglich eine Anonymisierung/Pseudonymisierung durchgeführt wird.
2. Maßnahmen, um die laufende Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz der Verarbeitungssysteme und -dienste sicherzustellen
 - a) Ein Sicherheitsbeauftragter oder ein designiertes Mitglied der Geschäftsleitung wird ernannt, der/das für die Koordinierung und Überwachung der Regeln und Verfahren zur Informationssicherheit verantwortlich ist.
 - b) Datenschutzaspekte werden als integraler Bestandteil des Unternehmensrisikomanagements etabliert.
 - c) Es werden für die Einrichtungen, in denen die personenbezogene Daten verarbeitenden Systeme untergebracht sind, Notfall- und Krisenpläne aufrechterhalten.
 - d) Gegebenenfalls wird eine Beurteilung der Auswirkungen auf den Datenschutz (DPIA) durchgeführt.
 - e) Die Mitarbeiter werden geschult und zur Vertraulichkeit und Geheimhaltung der Daten verpflichtet.
 - f) Die Mitarbeiter werden über einschlägige Sicherheitsverfahren und ihre jeweiligen Rollen informiert.

- g) Die Mitarbeiter werden über die möglichen Folgen von Verstößen gegen Sicherheitsregeln und -verfahren informiert.
 - h) Es werden den Mitarbeitern Arbeitsanweisungen zur Zugangskontrolle, Kommunikationssicherheit und Betriebssicherheit zur Verfügung gestellt.
 - i) In den Arbeitsanweisungen sind die Sicherheitsmaßnahmen, einschlägigen Verfahren und Zuständigkeiten ausdrücklich beschrieben.
 - j) Alle Datenschutzvorschriften, -anweisungen und -leitlinien werden zentral dokumentiert und sind allen Beschäftigten zugänglich.
 - k) Für den Systembetrieb wichtige Komponenten werden zu jeder Zeit überwacht und in dem erforderlichen Umfang durch Schutzsysteme geschützt, um sie vor Feuer, Wasser, Luftfeuchtigkeit, Erschütterungen, Hitze, Kälte und unvorhergesehenen Stromausfällen zu schützen.
 - l) Für den Systembetrieb wichtige Komponenten können im Falle eines Ausfalls innerhalb der vorgeschriebenen Zeit ersetzt werden, z. B. durch Backup-Komponenten, RAID-Systeme oder Datenspiegelung.
 - m) Gegebenenfalls werden für Betriebssysteme und Daten gesonderte Partitionen genutzt.
3. Maßnahmen, um die Fähigkeit sicherzustellen, die Verfügbarkeit personenbezogener Daten und den Zugang dazu im Falle eines physischen oder technischen Vorfalls zeitnah wiederherzustellen
- a) Es wird eine auf der Menge der Daten und der Häufigkeit von Datenänderungen beruhende Backup-Strategie festgelegt.
 - b) Die Backup-Strategie ist darauf ausgelegt, personenbezogene Daten gemäß ihrem letzten Zustand vor dem Datenverlust oder der Vernichtung der Daten wiederherzustellen.
 - c) Die Backup-Systeme werden physisch von den Produktionssystemen getrennt.
 - d) Es werden für die Backup-Server dieselben Sicherheitsmaßnahmen angewandt wie für die Produktionsserver.
 - e) Die mit der Wiederherstellung von Daten betrauten Personen werden speziell für diese Aufgabe geschult.
4. Prozesse zur regelmäßigen Testung, Bewertung und Auswertung der Wirksamkeit der technischen und organisatorischen Maßnahmen, um die Verarbeitungssicherheit sicherzustellen (TOMS)
- a) Die TOMS-Wirksamkeit wird in festgelegten Abständen durch den „Datenimporteur“ getestet. Art und Häufigkeit dieser Tests werden gemäß der jeweiligen Maßnahme festgelegt.
 - b) Falls Tests zeigen, dass die TOMS nicht ausreichend umgesetzt wurden oder nicht die erforderliche Wirksamkeit aufweisen, werden angemessene Maßnahmen festgelegt und ergriffen.

- c) Falls die Überprüfung bestehender TOMS zeigt, dass diese nicht länger ausreichen (z. B. aufgrund neuer Bedrohungen), werden neue TOMS eingeführt.
 - d) Es werden eine oder mehrere Personen festgelegt, um die Wirksamkeit der TOMS kontinuierlich zu überwachen und die Tests und ggf. zu ergreifenden Maßnahmen zu koordinieren.
5. Maßnahmen zur Nutzeridentifizierung und -autorisierung
- a) Der Zugriff auf Informationssysteme wird durch branchenübliche Identifizierungs- und Authentifizierungsverfahren geschützt.
 - b) Datenspeichergeräte, Arbeitsstationen, Notebooks, Smartphones und Tablets werden mittels branchenüblicher Verschlüsselungsmethoden verschlüsselt.
 - c) Benutzerkonten und Benutzerrechte werden von festgelegten Personen (Administratoren) verwaltet.
 - d) Das restriktive, bedarfsgestützte Autorisierungskonzept der Datenbankrechte wird mit einer Mindestanzahl von Administratoren verwaltet.
 - e) Der Zugriff auf personenbezogene Daten ist auf Beschäftigte beschränkt, die im Rahmen ihrer jeweiligen Tätigkeitsfunktion oder Rolle ein berechtigtes Bedürfnis haben, auf diese personenbezogenen Daten zuzugreifen.
 - f) Daten, die für andere Zwecke erhoben wurden, können getrennt von anderen Daten verarbeitet werden.
 - g) Systemaktivitäten, die über den autorisierten Zugriff hinausgehen, werden verhindert.
 - h) Es werden Leitlinien zu den folgenden Themen entwickelt und umgesetzt: „sichere Passwörter“, „Löschung/Vernichtung“, „sauberer Schreibtisch“, „mobiles Endgerät“.
 - i) Nutzerkonten, die eine Authentifizierung zulassen, sind personengebunden und werden nur von einer einzigen Person genutzt.
 - j) Die Mitarbeiter sind angewiesen, administrative Sitzungen zu deaktivieren, wenn Sie das Betriebsgelände verlassen oder wenn Arbeitsstationen anderweitig unbesetzt sind.
 - k) Benutzerpasswörter bestehen aus mindestens acht Zeichen, darunter Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
 - l) Für den Zugriff auf wichtige Systeme wird eine Zwei-Faktor-Authentifizierung genutzt.
 - m) Dateivernichtung und/oder externe Zerstörung von Dateien erfüllen den Sicherheitsstandard der DIN 66399.
6. Maßnahmen zum Schutz von Daten während der Übermittlung
- a) Remote-Zugriff erfolgt nur über verschlüsselte Linien (VPN).

- b) Die elektronische Datenübertragung und die Übermittlung personenbezogener Daten erfolgen mittels branchenüblicher Verschlüsselungsmethoden. Für E-Mails wird dort, wo diese unterstützt wird, zumindest Leitungsverschlüsselung (TLS) verwendet.
 - c) Gegebenenfalls werden Signaturverfahren umgesetzt.
 - d) Es werden keine Daten an unbekannte Drittparteien übermittelt.
7. Maßnahmen zum Schutz von Daten während der Speicherung
- a) Der Zugriff auf bestimmte Daten ist auf diejenigen beschränkt, die diese Daten verarbeiten müssen. Dies wird über ein Nutzerautorisierungsmodell gesteuert.
 - b) Wo relevant werden unterschiedliche Kundendaten in unterschiedlichen Datenbanken gespeichert.
 - c) Externe Speichermedien, die sensible personenbezogene Daten enthalten, werden verschlüsselt und physisch gesichert.
 - d) Das Recht, Daten einzugeben, zu verändern und zu löschen, wird auf der Basis eines Autorisierungskonzepts gewährt.
 - e) Das Recht auf Löschung wird restriktiv gewährt.
8. Maßnahmen zur Sicherstellung der physischen Sicherheit von Standorten, an denen personenbezogene Daten verarbeitet werden
- a) Systeme und Dienste werden gegen versehentliche oder ungesetzliche Vernichtung, versehentlichen Verlust, Änderung, unbefugte Weitergabe oder unbefugten Zugriff geschützt.
 - b) Ein Einbruchsmeldesystem einschließlich eines Alarms rund um die Uhr ist installiert.
 - c) Außen- und partitionierende Innentüren werden durch Magnet- und Schließkontakte gesichert.
 - d) Schlüssel und Schlüsselkarten werden jeweils einzelnen Personen zugewiesen.
 - e) Der Eingang oder Empfang ist während der Arbeitszeiten jederzeit besetzt.
 - f) Gebäude und Eingänge werden kontinuierlich videoüberwacht.
 - g) Besucher werden stets von Beschäftigten begleitet.
 - h) Externes Personal wird sorgfältig ausgewählt.
 - i) Für Systeme, die von externen Dienstleistern untergebracht, gehostet und gewartet werden, wird von diesen Dienstleistern die Umsetzung und Aufrechterhaltung entsprechender Maßnahmen veranlasst.
9. Maßnahmen zur Sicherstellung der Protokollierung von Ereignissen
- a) Zugangsautorisierungen und Datenabfrage werden überwacht und protokolliert.
 - b) Die Zuteilung von Schlüsseln und Schlüsselkarten wird protokolliert.

- c) Der Zugang von Besuchern wird protokolliert.
 - d) Eingabe, Veränderung und Löschung von Daten werden protokolliert.
 - e) Datenwiederherstellungsbemühungen werden protokolliert.
 - f) Die Ergebnisse von Tests der TOMS-Wirksamkeit werden protokolliert.
 - g) Die Ergebnisse von Tests der Berichtsstruktur werden protokolliert.
 - h) Sicherheitsvorfälle und Verletzungen des Schutzes der Daten werden protokolliert. Es werden Aufzeichnungen geführt, die die Art der Verletzung des Schutzes der Daten, die Kategorien und ungefähre Zahl der betreffenden betroffenen Personen, die Kategorien und ungefähre Zahl der betreffenden personenbezogenen Datensätze, den Zeitraum, die Folgen der Verletzung des Schutzes der Daten, das Verfahren zur Datenwiederherstellung, die zur Abmilderung negativer Folgen ergriffenen Maßnahmen, die Namen der die Verletzung des Schutzes der Daten meldenden Personen und die Namen der Personen, an die die Verletzung des Schutzes der Daten gemeldet wurde, umfassen.
 - i) Die Protokolle ermöglichen die Rückverfolgbarkeit einzelner Nutzer und nicht von Nutzergruppen.
10. Maßnahmen zur Sicherstellung der Systemkonfiguration, einschließlich der Standardkonfiguration
- a) Es werden technische Maßnahmen ergriffen, um die betroffenen Personen in die Lage zu versetzen, ihr Recht auf Widerruf ihrer Einwilligung auf einfache Weise auszuüben.
 - b) Es werden in Standard- und individueller Software datenschutzfreundliche Grundeinstellungen verwendet.
11. Maßnahmen zu internen Steuerung und Verwaltung von IT und IT-Sicherheit
- a) Es sind auf Servern und Clients Antivirus-Software und eine Firewall installiert, um vermeiden zu helfen, dass bösartige Software unbefugten Zugriff auf Systeme erhält.
 - b) Es ist ein Eindringungserkennungssystem umgesetzt.
 - c) Ein formalisiertes Verfahren zum Umgang mit Sicherheitsvorfällen ist vorhanden.
 - d) Der Remote-Zugang durch externe Parteien wird überwacht.
 - e) IT-Hardware und -Software werden in festgelegten Abständen überprüft, um zu beurteilen, ob sie aus Sicherheitsgründen aktualisiert oder ersetzt werden müssen.
12. Maßnahmen zur Zertifizierung/Prüfungssicherheit von Prozessen und Produkten
- a) Die Notwendigkeit der Zertifizierung für Systeme und Produkte wird regelmäßig beurteilt.
 - b) Datensicherheitszertifizierungen (falls zutreffend) und -audits (einschließlich von Penetrationstests, je nach Sachlage) werden regelmäßig wiederholt.

13. Maßnahmen zur Sicherstellung der Datenminimierung

- a) Personenbezogene Daten werden nur in dem zur Erfüllung des beabsichtigten Zwecks erforderlichen Umfang erfasst.
- b) Die gespeicherten personenbezogenen Daten werden in Abständen überprüft und gelöscht, wenn sie nicht mehr verwendet werden und sofern rechtliche oder vertragliche Vorgaben die Löschung dieser personenbezogenen Daten nicht verhindern.

14. Maßnahmen zur Sicherstellung der Datenqualität

- a) Wo angemessen unterliegt die Dateneingabe Plausibilitätstests.
- b) Wo angemessen erhalten Nutzer die Gelegenheit zur Verifizierung eingegebener Daten.

15. Maßnahmen zur Sicherstellung der Begrenzung der Speicherdauer von Daten

- a) Wo angemessen und möglich werden Speicherungszeiträume festgelegt.
- b) Wo möglich und angemessen werden für Dokumente und Daten in produktiven Systemen automatisierte Archivierungsprotokolle genutzt.

16. Maßnahmen zur Sicherstellung der Rechenschaftspflicht

- a) Es ist ein formaler Prozess festgelegt, um Sicherheitsvorfällen und Verletzungen des Schutzes der Daten nachzugehen.
- b) Die Kontrollmechanismen in Bezug auf die Einhaltung der Datenschutzgrundsätze basieren auf den Vorgaben der einschlägigen Datenschutzgesetze.
- c) Die Berichtsstrukturen sind auf die Organisation der Gruppe und der jeweiligen Einheit abgestimmt und ermöglichen Reaktionen in einem angemessenen und, sofern vorliegend, rechtlich vorgesehenen Zeitrahmen.
- d) Die Effektivität der Berichtsstrukturen wird in vorgegebenen Abständen überprüft.
- e) Falls die Tests zeigen, dass die Berichtsstrukturen nicht ausreichend umgesetzt wurden oder nicht die erforderliche Effektivität haben, werden angemessene Maßnahmen festgelegt und ergriffen.

17. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und der Sicherstellung der Datenlöschung

- a) Die Zuständigkeiten bezüglich der Datenübertragbarkeit sind klar festgelegt.
- b) Es bestehen formalisierte Prozesse für Datenübertragungsersuchen.
- c) Datensätze können durch die Auswahlfunktionen des genutzten Systems ermittelt und separiert werden.
- d) Datenübertragungsersuchen werden unverzüglich an die richtigen Einheiten geschickt und umgehend bearbeitet, damit in jedem Fall die gesetzlichen Fristen eingehalten werden.

- e) Es werden angemessene Maßnahmen umgesetzt, um nach Kündigung des Rahmenvertrags die Entfernung personenbezogener Daten aus den Systemen des Anbieters sicherzustellen.
- f) Die für die Datenübertragbarkeit zuständigen Personen sind geschult und kompetent im Umgang mit Ersuchen bezüglich der Datenübertragbarkeit. Insbesondere ist klar festgelegt, welche Informationen offengelegt, übermittelt oder gelöscht werden müssen und welchen Ersuchen oder Teilen von Ersuchen nicht nachzukommen ist.
- g) Personenbezogene Daten werden in strukturierten, gängigen und maschinenlesbaren Formaten unter Einsatz sicherer Methoden übermittelt.