

This Data Processing Addendum ("**DPA**") is entered into between _____ ("**Customer**"), acting on its own behalf and as an agent for any Customer Affiliate, and iGrafx GmbH or the relevant iGrafx GmbH subsidiary or parent company that will perform the Services described in the DPA (each referred to as "**Vendor**") and forms part of the iGrafx agreements(s) under which iGrafx is performing the Services, specifically the relevant iGrafx Cloud Services Agreement located at <https://www.igrafx.com/company/legal/cloud-services-agreement> and, in the event iGrafx is performing related professional services, the relevant Professional Services Terms and Conditions located at <https://www.igrafx.com/company/legal/services-terms-conditions> (collectively "**Principal Agreement**"). This DPA sets for the agreement between Vendor and Customer for the Processing of Personal Data in connection with the Agreement pursuant to the requirements of applicable Data Protection Laws.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement. Except where the context requires otherwise, references in this DPA to the Principal Agreement are to the Principal Agreement as amended by, and including, this DPA.

1. Definitions

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "Contracted Processor" means Vendor or a Subprocessor;

1.1.2 "Customer Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the

Dieses Addendum zur Datenverarbeitung (Data Processing Addendum, „**DPA**“) wird zwischen der

(„Kunde“), die in eigenem Namen und als Beauftragte für ein verbundenes Unternehmen des Kunden handelt, und der iGrafx GmbH oder der jeweiligen Tochter- oder Muttergesellschaft der iGrafx GmbH, die die im DPA beschriebenen Services erbringt (jeweils als „Anbieter“ bezeichnet), geschlossen und ist Teil der iGrafx Vereinbarungen, auf deren Grundlage iGrafx die Services erbringt, insbesondere der entsprechenden Vereinbarung über iGrafx Cloud Services, die sich unter <https://www.igrafx.com/company/legal/cld-services-agreement> befindet, und für den Fall, dass iGrafx damit verbundene professionelle Dienstleistungen erbringt, der entsprechenden Geschäftsbedingungen für professionelle Services, die sich unter <https://www.igrafx.com/company/legal/services-terms-conditions> befinden (zusammen „**Hauptvereinbarung**“). Dieses DPA legt die Vereinbarung zwischen dem Anbieter und dem Kunden über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Vereinbarung gemäß den Anforderungen der geltenden Datenschutzgesetze fest.

In Anbetracht der hier dargelegten gegenseitigen Verpflichtungen vereinbaren die Parteien hiermit, dass die nachstehenden Bedingungen der Hauptvereinbarung als Addendum hinzugefügt werden. Sofern sich aus dem Zusammenhang nichts anderes ergibt, beziehen sich Verweise auf die Hauptvereinbarung in diesem DPA auf die Hauptvereinbarung in der durch dieses DPA geänderten Fassung einschließlich dieses DPA.

1. Definitionen

Die in diesem DPA verwendeten Begriffe haben die in diesem DPA festgelegte Bedeutung. Begriffe, die mit einem Großbuchstaben beginnen, die hier nicht anders definiert sind, haben die Bedeutung, die in der Hauptvereinbarung festgelegt wird. Mit Ausnahme der nachstehenden Änderungen bleiben die Bestimmungen der Hauptvereinbarung in vollem Umfang in Kraft und wirksam.

1.1 In diesem DPA haben die folgenden Begriffe die nachstehend angegebene Bedeutung und verwandte Begriffe sind entsprechend auszulegen:

1.1.1 „Auftragsverarbeiter“ steht für Anbieter oder einen Unterauftragsverarbeiter.

1.1.2 „Verbundenes Unternehmen des Kunden“ bezeichnet eine juristische Person, die Eigentümer des Kunden ist oder diesen kontrolliert, sich im Besitz oder unter der Kontrolle des Kunden oder unter gemeinsamer

power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.3 "Data Controller" means the natural or legal person, public authority or other body which determines the purposes and means of the processing of Personal Data.

1.1.4 "Data Processor" means the Vendor entity that Processes Personal Data on behalf of the Data Controller.

1.1.5 "Data Subject" means the person to who Personal Data relates.

1.1.6 "EEA" means the European Economic Area;

1.1.7 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.8 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.9 "Instruction(s)" means the written, documented instructions, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data. Instructions include the Agreement, the DPA, and applicable order forms.

1.1.10 "Personal Data" means any information provided or made available by Customer or its end users or other Customer personnel pursuant to the Services and Principal Agreement relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.1.11 "Process" or "Processing" means any operation or set of operations which performed by Vendor as part of the Services or provision thereof on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.1.12 "Restricted Transfer" means:

1.1.12.1 a transfer of Personal Data of Customer to a Contracted Processor; or

1.1.12.2 an onward transfer of Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer

Kontrolle oder im gemeinsamen Besitz des Kunden befindet, wobei Kontrolle definiert ist als der direkte oder indirekte Besitz der Befugnis, die Leitung und die Politik eines Unternehmens zu lenken oder zu veranlassen, sei es durch den Besitz von stimmberechtigten Wertpapieren, durch einen Vertrag oder auf andere Weise. „Datenschutzgesetze“ bezeichnet die Datenschutzgesetze der EU und, soweit anwendbar, die Datenschutzgesetze eines anderen Landes.

1.1.3 „Datenverantwortlicher“ ist die natürliche oder juristische Person, Behörde oder sonstige Stelle, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

1.1.4 „Datenverarbeiter“ ist der Anbieter, der personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet.

1.1.5 „Betroffene Person“ ist die Person, auf die sich die personenbezogenen Daten beziehen.

1.1.6 „EWR“ bezeichnet den Europäischen Wirtschaftsraum.

1.1.7 „EU-Datenschutzgesetze“ steht für die EU-Richtlinie 95/46/EG, wie sie in das innerstaatliche Recht der einzelnen Mitgliedstaaten umgesetzt wurde und von Zeit zu Zeit geändert, ersetzt oder abgelöst wird, einschließlich der DSGVO und der Gesetze zur Umsetzung oder Ergänzung der DSGVO.

1.1.8 „DSGVO“ steht für Datenschutz-Grundverordnung (Verordnung (EU) 2016/679).

1.1.9 „Anweisung(en)“ sind die schriftlichen, dokumentierten Anweisungen, die der Datenverantwortliche dem Auftragsverarbeiter erteilt und die diesen anweisen, eine bestimmte Handlung in Bezug auf personenbezogene Daten durchzuführen. Zu den Anweisungen gehören die Vereinbarung, das DPA und die entsprechenden Auftragsformulare.

1.1.10 „Personenbezogene Daten“ sind alle Informationen, die der Kunde oder seine Endbenutzer oder andere Mitarbeiter des Kunden im Rahmen der Services- und Hauptvereinbarung über eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) bereitstellen oder zugänglich machen; eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

1.1.11 „Verarbeiten“ oder „Verarbeitung“ ist jeder Vorgang oder jede Reihe von Vorgängen, die der Anbieter im Rahmen der Services oder deren Erbringung an personenbezogenen Daten vornimmt, unabhängig davon, ob dies mit automatisierten Mitteln geschieht oder nicht,

restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 12 below;

1.1.13 "Services" means the services and other activities to be supplied to or carried out by Vendor for Customer pursuant to the Principal Agreement;

1.1.14 "Standard Contractual Clauses" means the contractual clauses set out in Module 2 or Module 3 to the European Commission's Standard Contractual Clauses dated June 4, 2021 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection;

1.1.15 "Subprocessor" means any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors, appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Customer in connection with the Principal Agreement; and

1.1.16 "Vendor Affiliate" means a subsidiary of the Vendor that may perform or otherwise assist in the performance of Services under the Principal Agreement.

1.2 The terms, "Commission", "Member State", "Personal Data Breach", and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

wie z. B. das Erheben, Aufzeichnen, Ordnen, Strukturieren, Speichern, Anpassen oder Verändern, Abrufen, Auslesen, Nutzen, Offenlegen durch Übermittlung, Verbreitung oder sonstige Bereitstellung, Abgleichen oder Kombinieren, Einschränken, Löschen oder Vernichten.

1.1.12 „Eingeschränkte Übermittlung“ bedeutet:

1.1.12.1 eine Übermittlung personenbezogener Daten des Kunden an einen Auftragsverarbeiter oder

1.1.12.2 eine Übergabe personenbezogener Daten von einem Auftragsverarbeiter an einen anderen Auftragsverarbeiter oder zwischen zwei Niederlassungen eines Auftragsverarbeiters,

in jedem Fall, wenn eine solche Übermittlung ohne die nachstehend in Abschnitt 12 festlegenden Standardvertragsklauseln nach den Datenschutzgesetzen (oder nach den Bedingungen von Datenübermittlungsvereinbarungen, die zur Einhaltung der in den Datenschutzgesetzen festgelegten Beschränkungen für die Datenübermittlung getroffen wurden) verboten wäre.

1.1.13 „Services“ sind die Dienstleistungen und sonstigen Tätigkeiten, die der Anbieter gemäß der Hauptvereinbarung für den Kunden zu erbringen oder auszuführen hat.

1.1.14 „Standardvertragsklauseln“ bezeichnet die in Modul 2 oder Modul 3 der Standardvertragsklauseln der Europäischen Kommission vom 4. Juni 2021 festgelegten Vertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten;

1.1.15 „Unterauftragsverarbeiter“ bezeichnet jeden Dritten und jedes verbundene Unternehmen des Anbieters, ausgenommen jedoch ein Mitarbeiter des Anbieters oder eines seiner Subunternehmen, der bzw. das vom oder im Namen des Anbieters oder eines verbundenen Unternehmens des Anbieters mit der Verarbeitung personenbezogener Daten im Auftrag eines Kunden unter Berufung auf die Hauptvereinbarung beauftragt wird.

1.1.16 „Verbundenes Unternehmen des Anbieters“ ist ein Zweigunternehmen des Anbieters, das Leistungen im Rahmen der Hauptvereinbarung erbringt oder anderweitig an der Erbringung von Services mitwirkt.

1.2 Die Begriffe „Kommission“, „Mitgliedsstaat“, „Verletzung des Schutzes personenbezogener Daten“ und „Aufsichtsbehörde“ haben die gleiche Bedeutung wie in der DSGVO, und verwandte Begriffe sind entsprechend auszulegen.

1.3 Das Wort „einschließen“ ist so zu verstehen, dass es ohne Einschränkung einschließt, und verwandte Begriffe sind entsprechend auszulegen.

<p>2. Roles and Responsibilities</p> <p>2.1 With regard the Processing of Personal Data pursuant the Agreement, the Customer agrees that it is the Data Controller and Vendor is the Data Processor. The Customer also agrees and consents to Vendor's use of Sub-Processors as set out in Section 6 below.</p> <p>2.2 Within the scope of the Agreement and in its use of the Services, Data Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data including Article 25 of the GDPR. For the avoidance of doubt, Data Controller's Instructions for the Processing of Personal Data shall comply with all Data Protection Laws. Controller shall inform Data Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data. Data Controller is solely responsible for the accuracy and legality of Personal Data including the manner and means by which Personal Data was collected or otherwise acquired.</p>	<p>2. Rollen und Zuständigkeiten</p> <p>2.1 Im Hinblick auf die Verarbeitung personenbezogener Daten gemäß der Vereinbarung erklärt sich der Kunde damit einverstanden, dass er der Datenverantwortliche und der Anbieter der Datenverarbeiter ist. Der Kunde erklärt sich auch damit einverstanden, dass der Anbieter Unterauftragsverarbeiter einsetzt, wie in Abschnitt 6 unten dargelegt.</p> <p>2.2 Im Rahmen der Vereinbarung und bei der Nutzung der Services ist der Datenverantwortliche allein verantwortlich für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre hinsichtlich der Offenlegung und Übermittlung personenbezogener Daten an den Auftragsverarbeiter und die Verarbeitung personenbezogener Daten, einschließlich Artikel 25 der Datenschutzgrundverordnung. Um jeden Zweifel auszuschließen: Die Anweisungen des Datenverantwortlichen für die Verarbeitung personenbezogener Daten müssen allen Datenschutzgesetzen entsprechen. Der Datenverantwortliche informiert den Datenverarbeiter unverzüglich und umfassend über alle Fehler oder Unregelmäßigkeiten im Zusammenhang mit den gesetzlichen Bestimmungen zur Verarbeitung personenbezogener Daten. Der Datenverantwortliche ist allein für die Richtigkeit und Rechtmäßigkeit der personenbezogenen Daten verantwortlich, einschließlich der Art und Weise und der Mittel, mit denen die personenbezogenen Daten erhoben oder auf andere Weise beschafft wurden.</p>
<p>3. Processing of Personal Data</p> <p>3.1 Customer shall Process Personal Data for use with the Services in accordance with applicable Data Protection Laws and has and shall provide all notices and consents necessary to use the Services in accordance with applicable Data Protection Laws. Customer will indemnify and hold harmless Vendor and Vendor Affiliates against any losses or liabilities arising from a breach of this clause 3.1 or other provision of the DPA.</p> <p>3.2 Details of Processing are set forth in Annex 1 to this DPA as well as certain information regarding the Contracted Processors' Processing of the Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of</p>	<p>3. Verarbeitung personenbezogener Daten</p> <p>3.1 Der Kunde verarbeitet personenbezogene Daten zur Verwendung mit den Services in Übereinstimmung mit den geltenden Datenschutzgesetzen und wird alle Mitteilungen und Einverständniserklärungen vorlegen, die für die Nutzung der Services in Übereinstimmung mit den geltenden Datenschutzgesetzen erforderlich sind. Der Kunde entschädigt und hält den Anbieter und die mit ihm verbundenen Unternehmen schadlos gegen jegliche Verluste oder Verbindlichkeiten, die sich aus einem Verstoß gegen diesen Abschnitt 3.1 oder eine andere Bestimmung des DPA ergeben.</p> <p>3.2 Die Einzelheiten der Verarbeitung sind in Anhang 1 dieses DPA aufgeführt, ebenso wie bestimmte Informationen über die Verarbeitung personenbezogener Daten durch die Auftragsverarbeiter, wie sie in Artikel 28 Absatz</p>

<p>other Data Protection Laws). The parties acknowledge and agree that Vendor may update the description of Processing from time to time to reflect new products, features or functionality comprised within the Services. Vendor will update relevant documentation to reflect such changes.</p>	<p>3 der DSGVO (und möglicherweise in gleichwertigen Anforderungen anderer Datenschutzgesetze) vorgeschrieben sind. Die Parteien nehmen zur Kenntnis und stimmen zu, dass der Anbieter die Beschreibung der Verarbeitung von Zeit zu Zeit aktualisieren kann, um neue Produkte, Merkmale oder Funktionalitäten der Dienste widerzuspiegeln. Der Anbieter wird die entsprechende Dokumentation aktualisieren, um solche Änderungen widerzuspiegeln.</p>
<p>3.3 Vendor shall:</p>	<p>3.3 Der Anbieter verpflichtet sich zu Folgendem:</p>
<p>3.3.1 Process Personal Data in accordance with Customer’s Instructions and applicable Data Protection Laws; and</p>	<p>3.3.1 Verarbeitung personenbezogener Daten entsprechend den Anweisungen des Kunden und den geltenden Datenschutzgesetzen und:</p>
<p>3.3.2 If the Vendor believes that an Instruction infringes applicable Data Protection Laws, Vendor will inform Customer without undue delay. If Vendor cannot process Personal Data in accordance with the Instruction due to a legal requirement under applicable Data Protection Laws, Vendor will (i) promptly notify the Customer of the legal requirement before the relevant Processing to the extent permitted by the applicable Data Protection Laws; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Customer issues new instructions with which Vendor is able to comply. If this provision is invoked, Vendor will not be liable to the Customer under the Agreement for any failure to perform the Services until such time as the Customer issues new instructions in regard to the Processing.</p>	<p>3.3.2 Ist der Anbieter der Ansicht, dass eine Anweisung gegen geltende Datenschutzgesetze verstößt, informiert er den Kunden unverzüglich darüber. Wenn der Anbieter personenbezogene Daten aufgrund einer gesetzlichen Vorschrift gemäß den geltenden Datenschutzgesetzen nicht den Anweisungen entsprechend verarbeiten kann, informiert der Anbieter i) den Kunden vor der betreffenden Verarbeitung unverzüglich über die gesetzliche Vorschrift, soweit dies nach den geltenden Datenschutzgesetzen zulässig ist, und ii) stellt die gesamte Verarbeitung (mit Ausnahme der bloßen Speicherung und Aufrechterhaltung der Sicherheit der betroffenen personenbezogenen Daten) ein, bis der Kunde neue Anweisungen erteilt, die der Anbieter einhalten kann. Wenn der Anbieter diese Bestimmung geltend macht, haftet er dem Kunden gegenüber nicht für jede Nichterfüllung der Services, solange der Kunde keine neuen Anweisungen hinsichtlich der Verarbeitung erteilt.</p>
<p>3.4 Customer:</p>	<p>3.4 Der Kunde:</p>
<p>3.4.1 Instructs, for the purposes of Clause 5(a) of the Standard Contractual Clauses, Vendor and each Vendor Affiliate (and authorizes Vendor and each Vendor Affiliate to instruct each Subprocessor) to:</p>	<p>3.4.1 beauftragt im Sinne von Klausel 5 Buchstabe a der Standardvertragsklauseln den Anbieter und jedes verbundene Unternehmen des Anbieters (und ermächtigt den Anbieter und jedes verbundene Unternehmen des Anbieters, jeden Unterauftragsverarbeiter zu beauftragen):</p>
<p>(i) Process Personal Data including Processing (a) in accordance with the Agreement, relevant sales quotes, order forms, schedules and statements of work; (b) initiated by Customer or end users in their access, receipt or use of the</p>	<p>(i) personenbezogene Daten zu verarbeiten, einschließlich der Verarbeitung a) gemäß der Vereinbarung, den betreffenden Angeboten, Auftragsformularen, Zeitplänen und Leistungsbeschreibungen, b) auf Veranlassung</p>

<p>Services; (c) to perform and enable the access, delivery, improvement, performance, provision, procurement, and use of the Services; and (d) comply with other reasonable Instructions provided by Customer. Process Personal Data as required to comply with applicable binding legal requirements by responding to binding requests for the disclosure of information as required by local laws and (e) in particular, to transfer Personal Data to any country or territory including the United States of America, as reasonably necessary for the provision of the Services and consistent with the Principal Agreement.</p> <p>(ii) Upon request, Vendor will reasonably assist Customer with its obligations under applicable Data Protection Laws and Regulations, in so far as possible in connection with the Services, taking into account the nature of Vendor's Processing and the Personal Data available to Vendor. Vendor shall be obliged to provide such assistance only in so far that Customer's obligations cannot be met by Customer through other means. Customer shall be responsible for any costs arising from Vendor's provision of such assistance to the extent legally permitted; and</p> <p>(iii) intentionally omitted.</p> <p>3.4.2 The Customer affirms that the DPA, the Agreement and the relevant order forms are Customer's complete and final instructions to Vendor in relation to Personal Data. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate Instructions.</p> <p>4. Vendor and Vendor Affiliate Personnel</p> <p>Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Personal</p>	<p>des Kunden oder der Endbenutzer bei deren Zugang, Empfang oder Nutzung der Services, c) um den Zugang, die Lieferung, Verbesserung, Leistung, Bereitstellung, Beschaffung und Nutzung der Services durchzuführen und zu ermöglichen und d) andere angemessene Anweisungen des Kunden zu erfüllen. Er verarbeitet personenbezogene Daten, soweit dies erforderlich ist, um die geltenden verbindlichen rechtlichen Anforderungen zu erfüllen, indem er auf verbindliche Anfragen zur Offenlegung von Informationen gemäß den nationalen Bestimmungen reagiert und (e) insbesondere personenbezogene Daten in jedes Land oder Gebiet, einschließlich der Vereinigten Staaten von Amerika, zu übermitteln, soweit dies für die Erbringung der Dienstleistungen und im Einklang mit dem Hauptvertrag erforderlich ist</p> <p>(ii) Auf Anfrage unterstützt der Anbieter den Kunden in angemessener Weise bei der Erfüllung seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen und -bestimmungen soweit dies im Zusammenhang mit den Services möglich ist, wobei die Art der Verarbeitung durch den Anbieter und die dem Anbieter zur Verfügung stehenden personenbezogenen Daten berücksichtigt werden. Der Anbieter ist zu einer solchen Unterstützung nur insoweit verpflichtet, als die Verpflichtungen des Kunden nicht auf andere Weise erfüllt werden können. Der Kunde ist für alle Kosten verantwortlich, die durch die Bereitstellung einer solchen Unterstützung durch den Anbieter entstehen, soweit dies gesetzlich zulässig ist, und</p> <p>(iii) absichtlich ausgelassen.</p> <p>3.4.2 bestätigt, dass das DPA, die Vereinbarung und die entsprechenden Auftragsformulare die vollständigen und endgültigen Anweisungen des Kunden an den Anbieter in Bezug auf personenbezogene Daten darstellen. Die Weisungen werden zunächst in der Vereinbarung festgelegt und können später von Zeit zu Zeit durch gesonderte Anweisungen des Verantwortlichen geändert, ergänzt oder ersetzt werden.</p> <p>4. Mitarbeiter des Anbieters und der verbundenen Unternehmen des Anbieters</p> <p>Der Anbieter und jedes verbundene Unternehmen des Anbieters ergreifen angemessene Maßnahmen, um die</p>
--	---

<p>Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.</p>	<p>Zuverlässigkeit aller Mitarbeiter, Bevollmächtigten oder Auftragnehmer eines Auftragsverarbeiters, die Zugang zu den personenbezogenen Daten haben, zu gewährleisten, wobei in jedem Fall sichergestellt wird, dass der Zugang strikt auf die Personen beschränkt ist, die die betreffenden personenbezogenen Daten kennen oder auf sie zugreifen müssen, soweit dies für die Zwecke der Hauptvereinbarung unbedingt erforderlich ist, und um die geltenden Gesetze im Zusammenhang mit den Pflichten dieser Personen gegenüber dem Auftragsverarbeiter einzuhalten, wobei sichergestellt wird, dass alle diese Personen einer Vertraulichkeitsverpflichtung oder einer beruflichen oder gesetzlichen Verschwiegenheitspflicht unterliegen.</p>
<p>5. Security</p>	<p>5. Sicherheit</p>
<p>5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR in accordance with Vendor's security standards described in Annex II to this DPA. Customer acknowledges that such security measures are subject to change due to technical progress and development and that Vendor and Vendor Affiliates may update or modify its security measures so long as such updates and modifications do not diminish the overall security of Vendor's Services. .</p>	<p>5.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie die unterschiedlich wahrscheinliche und schwerwiegende Gefahr für die Rechte und Freiheiten natürlicher Personen setzen der Anbieter und jedes mit ihm verbundene Unternehmen in Bezug auf die personenbezogenen Daten geeignete technische und organisatorische Maßnahmen um, um ein dieser Gefahr angemessenes Sicherheitsniveau zu gewährleisten, gegebenenfalls einschließlich der in Artikel 32 Absatz 1 der DSGVO genannten Maßnahmen gemäß den in Anhang II dieser DPA beschriebenen Sicherheitsstandards des Anbieters. Der Kunde nimmt zur Kenntnis dass sich diese Sicherheitsmaßnahmen aufgrund des technischen Fortschritts und der Entwicklung ändern können und dass der Anbieter und die verbundenen Unternehmen des Anbieters ihre Sicherheitsmaßnahmen aktualisieren oder modifizieren können, solange diese nicht die Gesamtsicherheit der Dienste des Anbieters beeinträchtigen.</p>
<p>5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.</p>	<p>5.2 Bei der Beurteilung des angemessenen Sicherheitsniveaus berücksichtigen der Anbieter und jedes mit ihm verbundene Unternehmen insbesondere die Risiken, die sich aus der Verarbeitung ergeben, insbesondere aus einer Verletzung des Schutzes personenbezogener Daten.</p>

<p>6. Subprocessing</p> <p>6.1 Customer (on behalf of itself and each Customer Affiliate) authorizes Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 6 to appoint) Subprocessors in accordance with this section 6. Vendor’s affiliates may also be retained as Subprocessors pursuant to Clause 5(h) of the standard Contractual Clauses. Vendor shall be liable for the acts and omissions of its Subprocessors to the same extent Vendor would be liable if performing the Services of each Subprocessor directly under the terms of the DPA, except as otherwise set forth in the Agreement.</p> <p>6.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this DPA. The Customer’s authorization in 6.1 above constitutes Controller’s prior written consent to the sub-Processing by Processor for purposes of Clause 11 of the Standard Contractual Clauses. A current list of Vendor’s Subprocessors is published at www.igrafx.com/legal/subprocessors and in Annex 3. Changes to Subprocessors will be reflected as updates to this list and Vendor shall provide notice to Customer of changes as set forth in Section 6.3 below</p> <p>Vendor shall give Customer prior written notice of the appointment of any new Subprocessor, including (i) the identity of the Subprocessor; and (ii) details of the Processing to be undertaken by the Subprocessor. Customer shall have the opportunity to object in writing to the appointment, within 10 days of receipt of Vendor’s notice, on reasonable grounds to the appointment (for example, if the Customer proves that Processing undertaken by the new Subprocessor would pose a significant risk for the protection of its Personal Data would exist or would violate applicable Data Protection Laws). If the Customer does not object within the relevant 10-day period, the new Subprocessor may be appointed. If the Customer wishes to object to the appointment of a new Subprocessor, Customer shall promptly notify Vendor, in writing, of its reasonable objection(s) which must specifically state specific reasons for the objection as well as possible mitigation options if available. If Vendor and Customer are unable to resolve such reasonable objections, either party may terminate the Services which cannot be provided</p>	<p>6. Vergabe eines Unterauftrags</p> <p>6.1 Der Kunde (im eigenen Namen und im Namen jedes mit ihm verbundenen Unternehmens) ermächtigt den Anbieter und jedes mit dem Anbieter verbundene Unternehmen, gemäß diesem Abschnitt 6 Unterauftragsverarbeiter zu ernennen und jedem gemäß diesem Abschnitt 6 ernannten Unterauftragsverarbeiter zu gestatten, Unterauftragsverarbeiter zu ernennen. Die verbundenen Unternehmen des Anbieters können auch als Unterauftragsverarbeiter gemäß Klausel 5 Buchstabe h der Standardvertragsklauseln eingesetzt werden. Der Anbieter haftet für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter in demselben Umfang, in dem er haften würde, wenn er die Services des jeweiligen Unterauftragsverarbeiters gemäß den Bedingungen des DPA direkt erbringen würde, sofern in der Vereinbarung nichts anderes festgelegt ist.</p> <p>6.2 Der Anbieter und jedes mit ihm verbundene Unternehmen können weiterhin die Unterauftragsverarbeiter nutzen, die der Anbieter oder ein mit ihm verbundenes Unternehmen zum Zeitpunkt der Unterzeichnung dieses DPA bereits beauftragt hatte. Die Autorisierung des Kunden unter 6.1 oben stellt die vorherige schriftliche Zustimmung des Datenverantwortlichen zur Unterverarbeitung durch den Auftragsverarbeiter im Sinn von Klausel 11 der Standardvertragsklauseln dar. Eine aktuelle Liste der Unterauftragsverarbeiter des Anbieters wird auf www.igrafx.com/legal/subprocessors und in Anhang 3 veröffentlicht. Änderungen der Unterauftragsverarbeiter werden als Aktualisierungen dieser Liste berücksichtigt, und der Anbieter muss den Kunden gemäß Abschnitt 6.3 über Änderungen informieren.</p> <p>Der Anbieter muss den Kunden vorab schriftlich über die Ernennung eines neuen Unterauftragsverarbeiters informieren, einschließlich (i) der Identität des Unterauftragsverarbeiters und (ii) Einzelheiten zu der vom Unterauftragsverarbeiter durchzuführenden Verarbeitung. Der Kunde hat die Möglichkeit, innerhalb von 10 Tagen nach Erhalt der Mitteilung des Anbieters schriftlich Widerspruch gegen die Ernennung einzulegen, sofern er dafür triftige Gründe vorbringen kann (z. B. wenn der Kunde nachweisen kann, dass die</p>
--	---

<p>by Vendor without the use of the Subprocessor by providing written notice to the other party. Customer, as its sole remedy, shall receive a refund of any prepaid but unused fees for such terminated Services for the remainder of the applicable Services term following the effective date of termination.</p>	<p>vom neuen Unterauftragsverarbeiter durchgeführte Verarbeitung ein erhebliches Risiko für den Schutz seiner personenbezogenen Daten darstellen oder gegen geltende Datenschutzgesetze verstoßen würde). Wenn der Kunde innerhalb der entsprechenden Frist von 10 Tagen keinen Widerspruch einlegt, kann der neue Unterauftragsverarbeiter ernannt werden. Wenn der Anbieter und der Kunde solche berechtigten Einwände nicht ausräumen können, kann jede Partei die Dienste, die vom Anbieter ohne den Einsatz des Unterauftragsverarbeiters nicht erbracht werden können, durch schriftliche Mitteilung an die andere Partei kündigen. Als einzige Abhilfe erhält der Kunde eine Rückerstattung aller im Voraus bezahlten, aber nicht in Anspruch genommenen Gebühren für solche gekündigten Dienste für die verbleibende Laufzeit der betreffenden Dienste nach dem Datum des Inkrafttretens der Kündigung.</p>
<p>7. Data Subject Rights</p> <p>7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate will provide reasonable assistance to Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligations, as reasonably understood by Vendor, to respond to requests to exercise Data Subject rights under the Data Protection Laws (such as access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Vendor, Vendor will promptly inform Customer and will advise Data Subjects to submit their request to the Customer. Customer shall be solely responsible for responding to any Data Subjects' requests. Customer shall reimburse Vendor for the costs arising from this assistance.</p>	<p>7. Rechte der betroffenen Personen</p> <p>7.1 Unter Berücksichtigung der Art der Verarbeitung werden der Anbieter und alle mit ihm verbundenen Unternehmen den Kunden in angemessener Weise unterstützen, indem sie geeignete technische und organisatorische Maßnahmen ergreifen, soweit dies möglich ist, um die Verpflichtungen des Kunden, wie sie der Anbieter vernünftigerweise versteht, zu erfüllen, um auf Anfragen zur Ausübung der Rechte der betroffenen Person gemäß den Datenschutzgesetzen (wie z. B. Zugang, Berichtigung, Einschränkung, Löschung oder Übertragbarkeit personenbezogener Daten, soweit anwendbar) zu reagieren, soweit dies gesetzlich zulässig ist. Wird eine solche Anfrage direkt an den Anbieter gerichtet, informiert der Anbieter den Kunden unverzüglich und rät den betroffenen Personen, ihre Anfrage an den Kunden zu richten. Der Kunde ist allein für die Beantwortung der Anfragen von betroffenen Personen verantwortlich. Der Kunde erstattet dem Anbieter die Kosten, die durch diese Unterstützung entstehen.</p>

<p>8. Personal Data Breach</p> <p>8.1 To the extent permitted by applicable law, Vendor shall notify Customer without undue delay upon Vendor becoming aware of a Personal Data Breach affecting Customer's Personal Data, and provide Customer with sufficient information to allow Customer to meet obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.</p> <p>8.2 At the Customer's request, Vendor will promptly provide the Customer with reasonable assistance as necessary to assist the Controller to report relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Vendor is required to do so under the Data Protection Laws.</p> <p>8.3 Vendor shall make reasonable efforts to identify and remediate the cause of the relevant Personal Data Breach shall make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as Vendor deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach to the extent the remediation is within Vendor's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer, Customer's affiliates or end users.</p>	<p>8. Verletzung des Schutzes personenbezogener Daten</p> <p>8.1 Soweit dies nach geltendem Recht zulässig ist, benachrichtigt der Anbieter den Kunden unverzüglich, sobald er von einer Verletzung des Schutzes personenbezogener Daten erfährt, die die personenbezogenen Daten des Kunden betrifft, und stellt dem Kunden ausreichende Informationen zur Verfügung, damit der Kunde seinen Verpflichtungen zur Meldung oder Information der betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten gemäß den Datenschutzgesetzen nachkommen kann.</p> <p>8.2 Auf Anfrage des Kunden bietet der Anbieter dem Kunden unverzüglich angemessene Unterstützung, um den Datenverantwortlichen dabei zu unterstützen, relevante Verstöße gegen den Schutz personenbezogener Daten den zuständigen Behörden und/oder den betroffenen Personen zu melden, wenn der Anbieter nach den Datenschutzgesetzen dazu verpflichtet ist.</p> <p>8.3 Der Anbieter unternimmt angemessene Anstrengungen, um die Ursache für die betreffende Verletzung des Schutzes personenbezogener Daten zu ermitteln und zu beheben, und ergreift die Schritte, die er für notwendig und angemessen hält, um die Ursache für eine solche Verletzung des Schutzes personenbezogener Daten zu beheben, soweit die Behebung in seinem Einflussbereich liegt. Die hierin enthaltenen Verpflichtungen gelten nicht für Vorfälle, die durch den Kunden, seine mit ihm verbundenen Unternehmen oder Endbenutzer verursacht werden.</p>
<p>9. Confidentiality</p> <p>9.1 Vendor shall ensure that its employees and contractors who undertake Processing of Personal Data are informed of the confidential nature of the Personal Data and are bound by obligations of confidentiality.</p>	<p>9. Vertraulichkeit</p> <p>9.1 Der Anbieter stellt sicher, dass seine Mitarbeiter und Auftragnehmer, die personenbezogene Daten verarbeiten, über die Vertraulichkeit der personenbezogenen Daten informiert werden und zur Verschwiegenheit verpflichtet sind.</p>
<p>10. Deletion of Personal Data</p> <p>10.1 Vendor shall delete Personal Data once such Personal Data is no longer needed for the purposes for which it was collected or upon the Instruction of Customer if the Customer is not able</p>	<p>10. Löschung personenbezogener Daten</p> <p>10.1 Der Anbieter löscht personenbezogene Daten, sobald diese für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden, oder auf Anweisung des Kunden, wenn der Kunde nicht in der Lage ist, diese personenbezogenen Daten</p>

<p>to directly delete such Personal Data from the Services. Certification of deletion of Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided by the Vendor (as Data Importer) to the Customer (as Data Exporter) only upon Customer's written request.</p>	<p>direkt aus den Services zu löschen. Eine Bescheinigung über die Löschung personenbezogener Daten gemäß Klausel 12 Absatz 1 der Standardvertragsklauseln stellt der Anbieter (als Datenimporteur) dem Kunden (als Datenexporteur) nur auf dessen schriftliche Anfrage aus.</p>
<p>10.2 Each Contracted Processor may retain Personal Data to the extent required by applicable law and only to the extent and for such period as required by applicable law and always provided that Vendor and each Vendor Affiliate shall maintain the confidentiality of all such Personal Data and shall Process such Personal Data for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.</p>	<p>10.2 Jeder Auftragsverarbeiter darf personenbezogene Daten nur in dem Umfang und für den Zeitraum speichern, wie es das geltende Recht vorschreibt, und immer unter der Voraussetzung, dass der Anbieter und jedes mit ihm verbundene Unternehmen die Vertraulichkeit aller personenbezogenen Daten wahrt und diese personenbezogenen Daten nur für den Zweck bzw. die Zwecke verarbeitet, der bzw. die in dem geltenden Recht, das ihre Speicherung vorschreibt, festgelegt ist bzw. sind, und für keinen anderen Zweck.</p>
<p>11. Audit rights</p>	<p>11. Überprüfungsrechte</p>
<p>11.1 If required by the Data Protection Laws and subject to the confidentiality obligation of the Principal Agreement, sections 11.2 to 11.4, after receipt of written notice from Customer, Vendor and each Vendor Affiliate shall make available to Customer information to demonstrate Vendor's compliance with this DPA in the form of third party certifications or audit results, and shall allow for on-site audits, including inspections, of Vendor's premises by Customer or third party auditor (bound by confidentiality obligations at least as protective as the Principal Agreement) appointed by the Customer and reasonably acceptable to Vendor, in relation to the Processing of the Personal Data by the Contracted Processors. Customer shall promptly notify Vendor of and with information regarding any non-compliance discovered during the course of an audit or inspection.</p>	<p>11.1 Soweit nach den Datenschutzgesetzen erforderlich und vorbehaltlich der Vertraulichkeitsverpflichtung der Hauptvereinbarung, Abschnitte 11.2 bis 11.4, stellen der Anbieter und jedes mit ihm verbundene Unternehmen dem Kunden nach Erhalt einer schriftlichen Mitteilung des Kunden Informationen zum Nachweis der Einhaltung dieses DPA durch den Anbieter in Form von Zertifizierungen oder Überprüfungsergebnissen Dritter zur Verfügung und gestatten Vor-Ort-Prüfungen, einschließlich Kontrollen in den Räumlichkeiten des Anbieters durch den Kunden oder einen vom Kunden beauftragten und für den Anbieter akzeptablen Prüfer eines Dritten (der an Vertraulichkeitsverpflichtungen gebunden ist, die mindestens dem Schutz der Hauptvereinbarung entsprechen) in Bezug auf die Verarbeitung der personenbezogenen Daten durch die Auftragsverarbeiter. Der Kunde ist verpflichtet, den Anbieter unverzüglich über alle Verstöße zu informieren, die im Rahmen einer Überprüfung oder Kontrolle festgestellt werden.</p>
<p>11.2 Information and audit rights of the Customer only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).</p>	<p>11.2 Auskunfts- und Überprüfungsrechte des Kunden ergeben sich im Abschnitt 11.1 nur insoweit, als die Hauptvereinbarung ihm nicht anderweitig Auskunfts- und Überprüfungsrechte einräumt, die den einschlägigen datenschutzrechtlichen</p>

<p>11.3 Customer shall give Vendor or the relevant Vendor Affiliate reasonable written notice (but in no event less than 30 days' notice) of any audit or inspection to be conducted under section 11.1 and shall avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:</p>	<p>Anforderungen (ggf. einschließlich Artikel 28 Absatz 3 Buchstabe h der DSGVO) genügen.</p>
<p>11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;</p> <p>11.3.2 outside normal business hours at those premises; or</p> <p>11.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except as required by applicable Data Protection Laws or if occasion demands.</p>	<p>11.3 Der Kunde muss den Anbieter oder das betreffende verbundene Unternehmen des Anbieters in einer angemessenen Frist (aber auf keinen Fall weniger als 30 Tage im Voraus) schriftlich von jeder Überprüfung oder Kontrolle, die gemäß Abschnitt 11.1 durchgeführt wird, benachrichtigen und vermeiden, im Verlauf einer solchen Überprüfung oder Kontrolle Schäden, Verletzungen oder Störungen der Räumlichkeiten, der Ausrüstung, des Personals und des Geschäftsbetriebs des Auftragsverarbeiters, während sich sein Personal in dessen Räumlichkeiten aufhält, zu verursachen (oder, falls dies nicht möglich ist, diese zu minimieren). Der Auftragsverarbeiter muss für die Zwecke einer solchen Überprüfung oder Kontrolle keinen Zugang zu seinen Räumlichkeiten gewähren:</p>
<p>11.4 Customer shall reimburse Vendor for any time expended for any audit or inspection at Vendor's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of such auditor inspection, Customer and Vendor shall mutually agree upon the scope, timing, and duration of the audit or inspection in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Vendor.</p>	<p>11.3.1 einer Person, es sei denn, sie legt einen angemessenen Nachweis ihrer Identität und Befugnis vor,</p> <p>11.3.2 außerhalb der normalen Geschäftszeiten in diesen Räumlichkeiten oder</p> <p>11.3.3 für die Zwecke von mehr als einer Überprüfung oder Kontrolle in Bezug auf jeden Auftragsverarbeiter in einem Kalenderjahr, es sei denn, dies ist nach den geltenden Datenschutzgesetzen erforderlich oder sofern anlassbezogen geboten.</p> <p>11.4 Der Kunde erstattet dem Anbieter den Zeitaufwand für Überprüfung oder Kontrolle zu den jeweils gültigen Tarifen des Anbieters für professionelle Dienstleistungen, die dem Kunden auf Anfrage zur Verfügung gestellt werden. Vor Beginn einer solchen Überprüfung vereinbaren der Kunde und der Anbieter gemeinsam den Umfang, den Zeitpunkt und die Dauer der Überprüfung oder Kontrolle sowie die Höhe der vom Kunden zu tragenden Kostenerstattung. Alle Erstattungsätze müssen unter Berücksichtigung der vom Anbieter angewendeten Mittel angemessen sein.</p>

12. European Specific Provisions/Restricted Transfers	12. Spezifische europäische Bestimmungen/Eingeschränkte Übertragungen
<p>12.1 Subject to section 12.3, Customer and/or Customer Affiliate, (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") hereby enter into the relevant Standard Contractual module:</p> <p>12.1.1 In relation to transfers of Personal Data Processed in accordance with Sections 3.1 and 3.3 of this DPA, the EU SCCs shall apply as follows:</p> <p>12.1.1.1 Module 2 or Module 3 will apply as relevant.</p> <p>12.1.1.2 In Clause 7, the optional docking clause will not apply.</p> <p>12.1.1.3 In Clause 9, option 2 will apply and the time period for notices shall be as set forth in Section 6 of this DPA.</p> <p>12.1.1.4 In Clause 17, option 1 will apply and the EU SCC's will be governed by German law.</p> <p>12.1.1.5 In Clause 18(b), disputes shall be resolved before the courts of Germany.</p> <p>12.1.1.6 Annex 1 of the EU SCCs is deemed completed with the information set forth in Annex 1 of this DPA.</p> <p>12.1.1.7 Subject to Section 5.1 of this DPA, Annex II of the EU SCCs is deemed completed with the information set forth in Annex II of this DPA.</p> <p>12.1.2 In relation to transfers of Personal Data protected by the UK GDPR, the EU SCCs will also apply in accordance with subsection 12.1.1 above, with the following modifications:</p> <p>12.1.2.1 references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR.</p> <p>12.1.2.2 references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the</p>	<p>12.1 Vorbehaltlich Abschnitt 12.3 treten der Kunde und/oder das verbundene Kundenunternehmen (als „Datenexporteur“) und jeder Auftragsverarbeiter, sofern zutreffend, (als „Datenimporteur“) hiermit in das entsprechende Standardvertragsmodul ein:</p> <p>12.1.1 In Bezug auf Übermittlungen personenbezogener Daten, die gemäß den Abschnitten 3.1 und 3.3 dieses DPA verarbeitet werden, gelten die EU-SCCs wie folgt:</p> <p>12.1.1.1 Modul 2 oder Modul 3 gelten je nach Relevanz.</p> <p>12.1.1.2 In Klausel 7 findet die optionale Docking-Klausel keine Anwendung.</p> <p>12.1.1.3 In Klausel 9 gilt Option 2 und die Frist für Benachrichtigungen wird in Abschnitt 6 dieses DPA festgelegt.</p> <p>12.1.1.4 In Ziffer 17 gilt Option 1 und die EU SCC unterliegen deutschem Recht.</p> <p>12.1.1.5 In Klausel 18(b) werden Streitigkeiten vor den Gerichten in Deutschland beigelegt.</p> <p>12.1.1.6 Anhang 1 der EU-SCCs gilt mit den in Anhang 1 dieses DPA aufgeführten Informationen als abgeschlossen.</p> <p>12.1.1.7 Vorbehaltlich Abschnitt 5.1 dieses DPA gilt Anhang II der EU-SCC als mit den in Anhang II dieses DPA aufgeführten Informationen abgeschlossen.</p> <p>12.1.2 In Bezug auf die Übermittlung personenbezogener Daten, die durch die britische GDPR geschützt sind, gelten die EU-SCCs auch gemäß Unterabschnitt 12.1.1 oben, mit den folgenden Änderungen:</p> <p>12.1.2.1 Verweise in den EU-SCCs auf „Richtlinie 95/46/EG“ oder „Verordnung (EU) 2016/679“ sind als Verweise auf die britische GDPR auszulegen; Verweise auf bestimmte Artikel der „Verordnung (EU) 2016/679“ werden durch den entsprechenden Artikel oder Abschnitt der britischen GDPR ersetzt.</p> <p>12.1.2.2 Verweise auf „EU“, „Union“ und „Recht der Mitgliedstaaten“ werden alle durch „UK“ ersetzt; Klausel 13(a) und Teil C von Anhang I der EU-SCCs werden nicht verwendet; Verweise auf die „zuständige Aufsichtsbehörde“ und „zuständige Gerichte“ sind als</p>

<p>Information Commissioner and the courts of England and Wales.</p> <p>12.1.2.3 Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts".</p> <p>If the EU SCCs, as described above, cannot be used to lawfully transfer such Personal Data in compliance with the UK GDPR then the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. In such a case the relevant annexes or appendices of the UK SCCs shall be populated using the information contained in Annex I and II of this DPA.</p> <p>12.1.3 In relation to transfers of Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with subsection 12.1.1 above, with the following modifications:</p> <p>12.1.3.1 references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;</p> <p>12.1.3.2 references to "EU", "Union" and "Member State law" are all replaced with Switzerland and Swiss law as relevant.</p> <p>12.1.3.3 References to "competent supervisory authority" shall be interpreted as a reference to the Swiss Federal Data Protection and Information Commission. References to "competent courts" shall be interpreted as a reference to competent courts located in Switzerland.</p> <p>If the EU SCCs, as described above, cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA then the Swiss SCC's shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. In such a case the relevant annexes or appendices of the Swiss SCCs shall be populated using the information contained in Annex I and II of this DPA.</p>	<p>Verweise auf den Information Commissioner und die Gerichte von England und Wales auszulegen.</p> <p>12.1.2.3 Klausel 17 der EU-SCCs wird ersetzt durch „Die Klauseln unterliegen dem Recht von England und Wales“ und Klausel 18 der EU-SCCs wird ersetzt durch „Jede Streitigkeit, die sich aus diesen Klauseln ergibt, wird von den Gerichte von England und Wales. Eine betroffene Person kann den Datenexporteur und/oder Datenimporteur vor den Gerichten eines beliebigen Landes im Vereinigten Königreich verklagen. Die Parteien vereinbaren, sich der Gerichtsbarkeit dieser Gerichte zu unterwerfen“.</p> <p>Wenn die EU-SCCs, wie oben beschrieben, nicht verwendet werden können, um solche personenbezogenen Daten in Übereinstimmung mit der britischen GDPRrechtmäßig zu übertragen, werden die UK-SCCs stattdessen durch Bezugnahme aufgenommen und bilden einen integralen Bestandteil dieses DPA und gelten für solche Übertragungen. In einem solchen Fall werden die entsprechenden Anhänge oder Anhänge der britischen SCCs unter Verwendung der in den Anhängen I und II dieser DPA enthaltenen Informationen ausgefüllt.</p> <p>12.1.3 In Bezug auf Übermittlungen von personenbezogenen Daten, die durch die Schweizer Datenschutzbehörde geschützt sind, gelten die EU-SCCs auch gemäß Unterabschnitt 12.1.1 oben, mit den folgenden Änderungen:</p> <p>12.1.3.1 Verweise in den EU-SCCs auf „Richtlinie 95/46/EG“ oder „Verordnung (EU) 2016/679“ sind als Verweise auf das Schweizerische Datenschutzgesetz auszulegen.</p> <p>12.1.3.2 Verweise auf „EU“, „Union“ und „Recht der Mitgliedstaaten“ werden alle durch die Schweiz und das schweizerische Recht ersetzt.</p> <p>12.1.3.3 Verweise auf „zuständige Aufsichtsbehörde“ sind als Verweis auf die Eidgenössische Datenschutz- und Informationskommission zu verstehen. Verweise auf „zuständige Gerichte“ sind als Verweis auf zuständige Gerichte mit Sitz in der Schweiz auszulegen.</p> <p>Wenn die EU-SCCs, wie oben beschrieben, nicht verwendet werden können, um solche personenbezogenen Daten in Übereinstimmung mit dem Schweizer DSG rechtmäßig zu übertragen, werden die Schweizer SCCs stattdessen durch Bezugnahme aufgenommen und bilden einen integralen Bestandteil dieses DSG und gelten für solche Übertragungen. In einem solchen Fall werden die entsprechenden Anhänge oder Anhänge der schweizerischen SCCs mit den</p>
--	---

<p>12.1.4 It is not the intention of the Providers to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses however, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses shall prevail to the extent of such conflict.</p> <p>12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:</p> <p>12.2.1 the data exporter (Customer) becoming a party to them;</p> <p>12.2.2 the data importer (Vendor) becoming a party to them; and</p> <p>12.2.3 commencement of the relevant Restricted Transfer.</p> <p>12.3 The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive or the GDPR, once effective) and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses apply when the Customer and Vendor have signed the Standard Contractual Clauses, where the Customer is established in the EEA or Switzerland as Data Controller and use of the Services by Customer or its end users results in the Personal Data of its Data Subjects being transferred to Vendor. For the purposes of this section and the Standard Contractual Clauses, the Customer is the Data Exporter and Vendor or the Vendor affiliate receiving Personal Data from the Data Exporter is the Data Importer.</p>	<p>Informationen aus den Anhängen I und II dieses DSGVO ausgefüllt.</p> <p>12.1.4 Der Anbieter beabsichtigt nicht, den Bestimmungen der Standardvertragsklauseln zu widersprechen oder diese einzuschränken, wenn und soweit die Standardvertragsklauseln mit einer Bestimmung der Vereinbarung (einschließlich dieser DPA) kollidieren, die Standardvertragsklauseln haben im Umfang eines solchen Konflikts Vorrang.</p> <p>12.2 Die Standardvertragsklauseln treten gemäß Abschnitt 12.1, je nachdem was später eintritt, in Kraft:</p> <p>12.2.1 der Datenexporteur (Kunde) wird Vertragspartei dieser Vertragsklauseln,</p> <p>12.2.2 der Datenimporteur (Anbieter) wird Vertragspartei dieser Vertragsklauseln und</p> <p>12.2.3 Beginn der jeweiligen eingeschränkten Übermittlung.</p> <p>12.3 Die Standardvertragsklauseln gelten nur für personenbezogene Daten, die aus dem Europäischen Wirtschaftsraum (EWR) entweder direkt oder im Wege der Weiterübermittlung an ein Land oder einen Empfänger außerhalb des EWR übermittelt werden, i) das/der von der Europäischen Kommission nicht als Land bzw. Empfänger anerkannt wird, das/der ein angemessenes Schutzniveau für personenbezogene Daten bietet (wie in der EU-Datenschutzrichtlinie oder DSGVO beschrieben, sobald diese in Kraft tritt), und ii) das/der nicht durch einen geeigneten Rahmen abgedeckt ist, der von den zuständigen Behörden oder Gerichten als angemessenes Schutzniveau für personenbezogene Daten anerkannt wird. Die Standardvertragsklauseln gelten, wenn der Kunde und der Anbieter die Standardvertragsklauseln unterzeichnet haben, wenn der Kunde im EWR oder in der Schweiz als Datenverantwortlicher ansässig ist und die Nutzung der Services durch den Kunden oder seine Endbenutzer dazu führt, dass die personenbezogenen Daten der betroffenen Personen an den Anbieter übermittelt werden. Im Sinne dieses Abschnitts und der Standardvertragsklauseln ist der Kunde der</p>
--	---

<p>13. Limitation of Liability</p> <p>Each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Customer, Customer's affiliates, and Vendor, whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Agreement and all DPAs together. For the avoidance of doubt, Vendor's and Vendor's Affiliates' total liability for all claims from the Customer and all of its affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Customer Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any affiliate that is a contractual party to any such DPA. Also, for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes.</p> <p>14. General Terms</p> <p>14.1 This DPA and Standard Contractual Clauses shall terminate automatically at the same time as the termination or expiration of the Principal Agreement. Additionally, Vendor may terminate this DPA and the Standard Contractual Clauses if Vendor offers the Customer an alternative that is compliant with applicable Data Protection Laws for the transfer of Personal Data outside the EEA or Switzerland to any country or entity not</p>	<p>Datenexporteur und der Anbieter oder das mit dem Anbieter verbundene Unternehmen, das personenbezogene Daten vom Datenexporteur erhält, der Datenimporteur.</p> <p>13. Haftungsbeschränkung</p> <p>Die gesamte Haftung aller Parteien und aller mit ihr verbundenen Unternehmen, die aus oder in Zusammenhang mit diesem DPA und allen zwischen dem Kunden, den verbundenen Unternehmen des Kunden und dem Anbieter abgeschlossenen DPA entsteht, unabhängig davon, ob sie sich aus einer Vereinbarung, einer unerlaubten Handlung oder aus einer anderen Haftungstheorie ergibt, unterliegt den Bestimmungen des Vertragsabschnitts zur Haftungsbeschränkung; mit jeder Bezugnahme auf die Haftung einer Partei, die in diesem Abschnitt erfolgt, ist die Gesamthaftung der Partei und aller mit ihr verbundenen Unternehmen gemeint, die sich auf die Vereinbarung und alle abgeschlossenen DPA zur Datenverarbeitung insgesamt begründet. Um jeden Zweifel auszuschließen, wird darauf hingewiesen, dass die Gesamthaftung des Anbieters und seiner verbundenen Unternehmen für alle Ansprüche des Kunden und aller seiner verbundenen Unternehmen, die sich aus der Vereinbarung und jedem DPA ergeben oder damit zusammenhängen, zu einer Gesamtheit aller Ansprüche aus der Vereinbarung und allen damit zusammenhängenden DPA zur Datenverarbeitung zusammengefasst und nicht als individuell oder einzeln für den Kunden und/oder verbundene Unternehmen des Kunden, der Vertragspartei eines solchen DPA ist, anwendbar verstanden werden sollen. Zur Klarstellung wird zudem darauf hingewiesen, dass jede Bezugnahme auf das DPA in diesem DPA auch die Anhänge des DPA mit einschließt.</p> <p>14. Allgemeine Bestimmungen</p> <p>14.1 Dieses DPA und die Standardvertragsklauseln enden automatisch zum gleichen Zeitpunkt wie die Kündigung oder der Ablauf der Hauptvereinbarung. Darüber hinaus kann der Anbieter dieses DPA und die Standardvertragsklauseln kündigen, wenn er dem Kunden eine Alternative anbietet, die den für die Übermittlung von personenbezogenen Daten außerhalb des EWR oder der Schweiz an ein Land oder eine Einrichtung, das/die laut</p>
--	--

<p>designated by the European Commission as providing an adequate level of protection for such transfer.</p>	<p>Festlegung der Europäischen Kommission kein angemessenes Schutzniveau für eine solche Übermittlung bereitstellt, geltenden Datenschutzgesetzen entspricht.</p>
<p>14.2 Unless prevented by applicable law, Each Customer Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, Customer Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Customer Affiliate must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Customer Affiliate shall be deemed a violation by Customer.</p>	<p>14.2 Sofern dies nicht durch geltendes Recht verhindert wird, jedes mit dem Kunden verbundene Unternehmen stimmt zu, an die Verpflichtungen aus diesem DPA und, soweit zutreffend, aus der Vereinbarung gebunden zu sein. Um jeden Zweifel auszuschließen, ist das verbundene Unternehmen des Kunden keine Vertragspartei und wird auch nicht zu einer solchen, sondern ist nur eine Partei des DPA. Jeglicher Zugang zu den Services und deren Nutzung durch das verbundene Unternehmen des Kunden muss den Bedingungen der Vereinbarung entsprechen und jede Verletzung der Bedingungen der Vereinbarung durch ein verbundenes Unternehmen des Kunden wird als Verletzung durch den Kunden betrachtet.</p>
<p>14.3 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:</p>	<p>14.3 Unbeschadet der Klauseln 7 (Schlichtungsverfahren und Gerichtsstand) und 9 (Anwendbares Recht) der Standardvertragsklauseln:</p>
<p>14.3.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and</p>	<p>14.3.1 Die Parteien dieses DPA unterwerfen sich hiermit der in der Hauptvereinbarung festgelegten Wahl des Gerichtsstands in Bezug auf alle Streitigkeiten oder Ansprüche, die sich aus diesem DPA ergeben, einschließlich Streitigkeiten über dessen Bestehen, Gültigkeit oder Beendigung oder die Folgen seiner Nichtigkeit, und</p>
<p>14.3.2 this DPA and all other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated in the Principal Agreement.</p>	<p>14.3.2 dieses DPA und alle anderen Verpflichtungen, die sich aus oder in Verbindung mit ihm ergeben, unterliegen dem Recht des Landes oder Gebiets, das in der Hauptvereinbarung angegeben ist.</p>
<p>14.4 Nothing in this DPA reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.</p>	<p>14.4 Keine Bestimmung dieses DPA schränkt die Verpflichtungen des Anbieters oder eines mit ihm verbundenen Unternehmens im Rahmen der Hauptvereinbarung in Bezug auf den Schutz personenbezogener Daten ein oder gestattet dem Anbieter oder einem mit ihm verbundenen Unternehmen, personenbezogene Daten in einer Weise zu verarbeiten (oder deren Verarbeitung zuzulassen), die nach der Hauptvereinbarung verboten ist. Im Fall eines Widerspruchs oder einer Unstimmigkeit zwischen diesem DPA und den</p>
<p>14.5 Subject to section 14.4, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Principal Agreement and including (except where</p>	<p></p>

<p>explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.</p>	<p>Standardvertragsklauseln haben die Standardvertragsklauseln Vorrang.</p>
<p>14.6 The Parties will work together in good faith to agree any amendments to this Addendum which either reasonably considers to be necessary to address the requirements of any change in Data Protection Laws.</p>	<p>14.5 Vorbehaltlich des Abschnitts 14.4 haben im Fall von Widersprüchen zwischen den Bestimmungen dieses DPA und anderen Vereinbarungen zwischen den Parteien, einschließlich der Hauptvereinbarung und einschließlich (sofern nicht ausdrücklich schriftlich anders vereinbart und im Namen der Parteien unterzeichnet) Vereinbarungen, die nach dem Datum dieses DPA abgeschlossen wurden oder angeblich abgeschlossen wurden, die Bestimmungen dieses DPA Vorrang.</p>
<p>14.7 Except as specifically amended and modified by this DPA, the terms and provisions of the Principal Agreement remain unchanged and in full force and effect. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.</p>	<p>14.6 Die Parteien werden nach Treu und Glauben zusammenarbeiten, um Änderungen dieses Addendums zu vereinbaren, die eine der Parteien vernünftigerweise für erforderlich hält, um den Anforderungen bei einer Änderung der Datenschutzgesetze gerecht zu werden.</p> <p>14.7 Sofern in diesem DPA nicht explizit ergänzt oder anders geregelt, bleiben die Bestimmungen der Hauptvereinbarung unverändert und rechtsgültig. Sollte eine Bestimmung dieses DPA ungültig oder nicht durchsetzbar sein, so bleiben die übrigen Bestimmungen dieses DPA gültig und in Kraft. Die unwirksame oder undurchsetzbare Bestimmung ist entweder i) so zu ändern, dass ihre Wirksamkeit und Durchsetzbarkeit gewährleistet ist, wobei die Absichten der Parteien so weit wie möglich erhalten bleiben, oder, falls dies nicht möglich ist, ii) so auszulegen, als ob der unwirksame oder undurchsetzbare Teil nie darin enthalten gewesen wäre.</p>

[DIE UNTERSCHRIFTEN ERSCHEINEN AUF DER NÄCHSTEN SEITE.]

ZU URKUND DESSEN wird dieses DPA unterzeichnet und mit Wirkung des oben genannten Datums verbindlicher Teil der Hauptvereinbarung.

NAME DES KUNDEN _____

Unterschrift:

Name:

Titel:

Datum der Unterzeichnung:

iGrafx GmbH

Unterschrift:

Name:

Titel:

Datum der Unterzeichnung:

<p>Data Exporter's and its affiliates' employees, end users, contractors, advisors, subcontractors, business partners who are natural persons.</p> <p>2. Categories of personal data transferred: employee names, work email addresses, work telephone numbers and work postal address, product types in use by data subjects</p> <p>3. Sensitive data transferred? None.</p> <p>4. The frequency of the transfer? Continuous.</p> <p>5. Nature of the processing: Providing products and services to end users.</p> <p>6. Purpose(s) of the data transfer and further processing: Providing products and services to end users.</p> <p>7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Upon termination of services, customer accounts are deactivated and deleted within sixty (60) days after the end of the customer's subscription term.</p> <p>8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As per 6 above, the sub-processors will process personal data as necessary to provide the products and services. The sub-processors used for the provision of products and services and their country of location are listed under the Annex III.</p> <p>C. COMPETENT SUPERVISORY AUTHORITY For the purposes of the Standard Contractual Clauses, the supervisory authority that shall act as competent supervisory authority is either (i) where data exporter is established in an EU Member State, the supervisory authority responsible for ensuring data exporter's compliance with the GDPR; (ii) where data exporter is not established in an EU Member State but falls within the extra-territorial scope of the GDPR and has appointed a</p>	<p>Mitarbeiter des Datenexporteurs und seiner verbundenen Unternehmen, Endbenutzer, Auftragnehmer, Berater, Subunternehmer, Geschäftspartner, die natürliche Personen sind.</p> <p>2. Kategorien der übermittelten personenbezogenen Daten: Mitarbeiternamen, geschäftliche E-Mail-Adressen, geschäftliche Telefonnummern und geschäftliche Postanschrift, durch die betroffenen Personen verwendete Produkttypen</p> <p>3. Sensible Daten übertragen? Keine.</p> <p>4. Die Häufigkeit der Übertragung? Kontinuierlich.</p> <p>5. Art der Verarbeitung: Bereitstellung von Produkten und Dienstleistungen für Endbenutzer.</p> <p>6. Zweck(e) der Datenübertragung und Weiterverarbeitung: Bereitstellung von Produkten und Dienstleistungen für Endbenutzer.</p> <p>7. Die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer: Bei Beendigung der Dienste werden Kundenkonten deaktiviert und innerhalb von sechzig (60) Tagen nach Ablauf der Abonnementlaufzeit des Kunden gelöscht.</p> <p>8. Bei Übermittlungen an (Unter-)Auftragsverarbeiter auch Gegenstand, Art und Dauer der Verarbeitung angeben: Die Unterauftragsverarbeiter verarbeiten gemäß vorstehender Ziffer 6 personenbezogene Daten, soweit dies zur Bereitstellung der Produkte und Dienstleistungen erforderlich ist. Die für die Erbringung von Produkten und Dienstleistungen eingesetzten Unterauftragsverarbeiter sowie deren Standort sind in Anhang III aufgeführt.</p> <p>C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE Im Sinne der Standardvertragsklauseln ist die Aufsichtsbehörde, die als zuständige Aufsichtsbehörde handelt, entweder (i) wenn der Datenexporteur seinen Sitz in einem EU-Mitgliedstaat hat, die für die Einhaltung der DSGVO durch den Datenexporteur zuständige Aufsichtsbehörde; (ii) wenn der Datenexporteur nicht in einem EU-Mitgliedstaat ansässig ist,</p>
---	--

<p>representative, the supervisory authority of the EU Member State in which data exporter's representative is established; or (iii) where data exporter is not established in an EU Member State but falls within the extra-territorial scope of the GDPR without having to appoint a representative, the supervisory authority of the EU Member State in which the data subjects are predominantly located. In relation to personal data that is subject to the UK GDPR or Swiss DPA, the competent supervisory authority is the UK Information Commissioner or the Swiss Federal Data Protection and Information Commissioner (as relevant).</p>	<p>aber in den extraterritorialen Anwendungsbereich der DSGVO fällt und einen Vertreter bestellt hat, die Aufsichtsbehörde des EU-Mitgliedstaats, in dem der Vertreter des Datenexporteurs niedergelassen ist; oder (iii) wenn der Datenexporteur seinen Sitz nicht in einem EU-Mitgliedstaat hat, aber in den extraterritorialen Anwendungsbereich der DSGVO fällt, ohne dass ein Vertreter bestellt werden muss, die Aufsichtsbehörde des EU-Mitgliedstaats, in dem sich die betroffenen Personen überwiegend befinden. In Bezug auf personenbezogene Daten, die der britischen DSGVO oder dem Schweizerischen Datenschutzgesetz unterliegen, ist die zuständige Aufsichtsbehörde der UK Information Commissioner oder der Eidgenössische Datenschutz- und Informationsbeauftragte (je nach Relevanz).</p>

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA/ANHANG II ZU DEN STANDARDVERTRAGSKLAUSELN

<p>Confidentiality of Personal Data Measures to ensure long-term confidentiality include: Confidentiality agreements with internal and external employees Confidentiality agreements with external service providers Security agreements with external service providers Use of a comprehensive data protection concept. Follow security policies to identify vulnerabilities for personal data protection and manage the security infrastructure. Definition and control of the use of authorized resources, in particular communication channels Protection against external influences (espionage, hacking) Specified environments equipped for data processing in accordance with the data protection concept (buildings, rooms, in detail server rooms) Consideration of the principles of data protection through technology and the privacy-friendly basic settings (privacy by design, privacy by default) in the data protection concept Limitation of the permissible personnel to those who have verifiable competence (local, technical), professionally qualified, reliable (if necessary safety-checked) and formally approved and have no conflicts of interest in the exercise Protection needs classification of personal data to be processed. Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Vertraulichkeit personenbezogener Daten Zu den Maßnahmen zur Gewährleistung der langfristigen Vertraulichkeit gehören: Vertraulichkeitsvereinbarungen mit internen und externen Mitarbeitern. Geheimhaltungsvereinbarungen mit externen Dienstleistern. Sicherheitsvereinbarungen mit externen Dienstleistern Einsatz eines umfassenden Datenschutzkonzeptes. Befolgen von Sicherheitsrichtlinien, um Schwachstellen für den Schutz personenbezogener Daten zu identifizieren und die Sicherheitsinfrastruktur zu verwalten. Definition und Kontrolle der Nutzung autorisierter Ressourcen, insbesondere Kommunikationskanäle. Schutz vor äußeren Einflüssen (Spionage, Hacking) Spezifizierte Umgebungen, die für die Datenverarbeitung gemäß dem Datenschutzkonzept ausgestattet sind (Gebäude, Räume, im Detail Serverräume). Berücksichtigung der Grundsätze des Datenschutzes durch Technik und der datenschutzfreundlichen Grundeinstellungen (Privacy by Design, Privacy by Default) im Datenschutzkonzept. Beschränkung des zulässigen Personals auf Personen, die über nachweisbare Kompetenz (lokal, technisch), fachlich qualifiziert, zuverlässig (ggf. sicherheitsgeprüft) und formell zugelassen sind und keine Interessenkonflikte in der Ausübung haben. Der Schutz erfordert eine Klassifizierung der zu verarbeitenden personenbezogenen Daten. Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Integrity of Personal Data The technical and organizational measures taken to protect against unauthorized or unlawful processing, destruction or unintentional damage include: Use of checksums, electronic seals and signatures in data processing processes according to the crypto concept. Document the assignment of permissions and roles. Processes to maintain up-to-dateness of data. Documentation of hardware and software inventory and management of an inventory Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Integrität personenbezogener Daten Zu den technischen und organisatorischen Maßnahmen zum Schutz vor unbefugter oder rechtswidriger Verarbeitung, Zerstörung oder unbeabsichtigter Beschädigung gehören: Verwendung von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen nach dem Kryptokonzept. Dokumentieren Sie die Vergabe von Berechtigungen und Rollen. Prozesse zur Aufrechterhaltung der Aktualität der Daten. Dokumentation des Hard- und Softwareinventars und Verwaltung eines Inventars. Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Pseudonymization Measures related to the pseudonymization of personal data. Pseudonymization of data according to a risk-based approach according to different protection requirements categories of data</p>	<p>Pseudonymisierung Maßnahmen zur Pseudonymisierung personenbezogener Daten. Pseudonymisierung von Daten nach einem risikobasierten Ansatz nach unterschiedlichen Schutzbedarfskategorien von Daten.</p>

<p>Encryption</p> <p>The encryption of personal data is a common way to protect it against unauthorized knowledge. In particular, encryption is suitable for preserving data from external influences such as hacking attacks and espionage. Encryption is a method by which a clearly legible information is converted into an unreadable or interpretable sequence of characters.</p> <p>Measures related to the encryption of personal data:</p> <p>Selection of an appropriate cryptographic method is carried out after taking into account the current state of the art and the protection requirements categories of the personal data to be processed.</p> <p>Use of encryption methods according to the data protection concept.</p> <p>Regular examination of encryption procedures (in case for security vulnerabilities) and adaptation of them to current technical developments (in s. updating the software used)</p> <p>Regular processing of archived encrypted data according to the latest state of the art (in case of the introduction of new encryption methods in data processing activities)</p> <p>Encryption policies take into account the different protection categories of personal data deletion of the original file after successful encryption; in the case of WORM media destruction of the entire data carrier.</p> <p>Processes for managing and protecting cryptographic information (in particular, the authorization concept for internal and external employees who have access to encrypted information)</p> <p>Training of internal and external employees in the handling of encrypted personal data (at least twice a year)</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Verschlüsselung</p> <p>Die Verschlüsselung personenbezogener Daten ist eine gängige Methode, um diese vor unberechtigter Kenntnisnahme zu schützen. Insbesondere eignet sich die Verschlüsselung, um Daten vor äußeren Einflüssen wie Hackerangriffen und Spionage zu schützen. Verschlüsselung ist ein Verfahren, bei dem eine gut lesbare Information in eine unlesbare oder interpretierbare Zeichenfolge umgewandelt wird.</p> <p>Maßnahmen im Zusammenhang mit der Verschlüsselung personenbezogener Daten:</p> <p>Die Auswahl eines geeigneten kryptographischen Verfahrens erfolgt unter Berücksichtigung des aktuellen Stands der Technik und des Schutzes der Kategorien der zu verarbeitenden personenbezogenen Daten.</p> <p>Einsatz von Verschlüsselungsverfahren nach dem Datenschutzkonzept.</p> <p>Regelmäßige Überprüfung von Verschlüsselungsverfahren (bei Sicherheitslücken) und Anpassung an aktuelle technische Entwicklungen (siehe s. Aktualisierung der eingesetzten Software)</p> <p>Regelmäßige Verarbeitung archivierter verschlüsselter Daten nach dem neuesten Stand der Technik (bei Einführung neuer Verschlüsselungsverfahren in der Datenverarbeitung)</p> <p>Verschlüsselungsrichtlinien berücksichtigen die verschiedenen Schutzkategorien der Löschung personenbezogener Daten der Originaldatei nach erfolgreicher Verschlüsselung; bei WORM-Medien Vernichtung des gesamten Datenträgers.</p> <p>Prozesse zur Verwaltung und zum Schutz kryptografischer Informationen (insbesondere das Berechtigungskonzept für interne und externe Mitarbeiter, die Zugriff auf verschlüsselte Informationen haben)</p> <p>Schulung interner und externer Mitarbeiter im Umgang mit verschlüsselten personenbezogenen Daten (mindestens zweimal jährlich)</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Availability</p> <p>Measures to ensure long-term availability:</p> <p>Central procurement of hardware and software</p> <p>Use of centrally tested and approved standard software from secure sources.</p> <p>Regular execution of data backups or use of mirroring procedures</p> <p>Decommissioning of hardware (in particular servers) takes place after a check of the data carriers used in it and, if necessary, after the relevant data records have been established.</p> <p>Uninterruptible Power Supply (UPS)</p> <p>Separate retention of data sets collected for different purposes or belonging to different categories of protection requirements.</p> <p>Multi-layered anti-virus and firewall architecture</p> <p>Emergency planning (emergency plan for security and data protection violations with concrete instructions)</p>	<p>Verfügbarkeit</p> <p>Maßnahmen zur Sicherstellung der Langzeitverfügbarkeit:</p> <p>Zentrale Beschaffung von Hard- und Software</p> <p>Einsatz von zentral geprüfter und freigegebener Standardsoftware aus sicheren Quellen.</p> <p>Regelmäßige Durchführung von Datensicherungen oder Einsatz von Spiegelungsverfahren</p> <p>Die Außerbetriebnahme von Hardware (insbesondere Servern) erfolgt nach Prüfung der darin verwendeten Datenträger und ggf. nach Erstellung der entsprechenden Datensätze.</p> <p>Unterbrechungsfreie Stromversorgung (USV)</p> <p>Getrennte Aufbewahrung von Datensätzen, die zu unterschiedlichen Zwecken erhoben wurden oder zu unterschiedlichen Kategorien von Schutzanforderungen gehören.</p> <p>Mehrschichtige Antiviren- und Firewall-Architektur</p>

<p>Fire/water and temperature early warning system in the server rooms Fire doors Support of IT by qualified and constantly trained employees Regular testing of data recovery according to the data protection concept</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure</p>	<p>Notfallplanung (Notfallplan für Sicherheits- und Datenschutzverstöße mit konkreten Anweisungen) Feuer-/Wasser- und Temperatur-Frühwarnsystem in den Serverräumen Feuer Türen Betreuung der IT durch qualifizierte und ständig geschulte Mitarbeiter Regelmäßige Prüfung der Datenwiederherstellung gemäß Datenschutzkonzept</p> <p>Kommentar: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt</p>
<p>Measures to ensure the resilience of systems and services in the long term: Dynamic processes and memory switching Penetration tests Regular stress tests of data processing systems Set the load limit for the respective data processing system in advance above the necessary minimum Regular training of deployed personnel (management and other internal and external staff) to act in accordance with the requirement to ensure the integrity and confidentiality of data processing (at least once a year)</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure</p>	<p>Maßnahmen zur langfristigen Sicherstellung der Belastbarkeit von Systemen und Diensten: Dynamische Prozesse und Speicherumschaltung Penetrationstests Regelmäßige Stresstests von Datenverarbeitungssystemen Stellen Sie die Belastungsgrenze für die jeweilige Datenverarbeitungsanlage vorab über das notwendige Minimum Regelmäßige Schulung des eingesetzten Personals (Führungskräfte und sonstiges internes und externes Personal) zum Handeln gemäß der Anforderung zur Wahrung der Integrität und Vertraulichkeit der Datenverarbeitung (mindestens einmal jährlich)</p> <p>Kommentar: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt</p>
<p>Recoverability of availability Measures to quickly restore availability in the event of a physical or technical incident: Regular archiving of data sets and use of mirroring methods. Separate retention of data assets Data Breach Management Plan Regularly test data recovery tools Emergency power supply Two independent access to the external network (Internet access from at least two different providers) Availability of back-up computers and software solutions for emergency situations</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Wiederherstellbarkeit der Verfügbarkeit Maßnahmen zur schnellen Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Vorfall: Regelmäßige Archivierung von Datensätzen und Einsatz von Spiegelungsmethoden. Getrennte Aufbewahrung von Datenbeständen Managementplan für Datenschutzverletzungen Testen Sie regelmäßig Datenwiederherstellungstools Notstromversorgung Zwei unabhängige Zugänge zum externen Netz (Internetzugang von mindestens zwei verschiedenen Anbietern) Verfügbarkeit von Backup-Computern und Softwarelösungen für Notfallsituationen</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Reviewing and evaluating data security Measures to review, evaluate and evaluate the effectiveness of technical and organizational measures on a regular basis: Internal and external audit reports and evaluations Regularly evaluate test results and adaptation measures Regular review of hardware and software inventory according to an inventory and annual update of the inventory Regular review of data processing systems and processing activities for vulnerabilities that may arise as a result of new</p>	<p>Überprüfung und Bewertung der Datensicherheit Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen: Interne und externe Auditberichte und Auswertungen Testergebnisse und Anpassungsmaßnahmen regelmäßig auswerten Regelmäßige Überprüfung des Hard- und Softwareinventars gemäß Inventarisierung und jährliche Aktualisierung des Inventars Regelmäßige Überprüfung von Datenverarbeitungssystemen und</p>

<p>technological developments or changing processing practices. Regular version control of standard software according to the data protection concept (intensity of control depends on the software used, but verification should be carried out at least once a year) Regular comparison of the protection requirements classification of the personal data to be processed with any new requirements of the controller.</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Verarbeitungsaktivitäten auf Schwachstellen, die sich aus neuen technologischen Entwicklungen oder sich ändernden Verarbeitungspraktiken ergeben können. Regelmäßige Versionskontrolle von Standardsoftware gemäß Datenschutzkonzept (Intensität der Kontrolle ist abhängig von der eingesetzten Software, jedoch sollte eine Verifizierung mindestens einmal jährlich erfolgen) Regelmäßiger Abgleich der schutzwürdigen Einstufung der zu verarbeitenden personenbezogenen Daten mit allfälligen neuen Anforderungen des Verantwortlichen.</p> <p>Kommentar: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt</p>
<p>Access 1: Measures to prevent access to personal data for unauthorized persons: Use user-related and customized credentials. Default for setting passwords (e.g. special characters, minimum length, regular password change) Prohibition of password sharing Authorization concept at the application and data level with differentiated authorization levels (profiles, roles, transactions and objects) Logging of assigned access permissions Use of signatures and certificates to ensure authorship and authorization for knowledge. Encryption of data and disks depending on their need for protection. Data protection-compliant destruction of data, data carriers and printouts according to protection class concept Prohibition of the use of private data carriers Policy for copying data. Access protection by screensavers</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Zugang 1: Maßnahmen zur Verhinderung des Zugriffs auf personenbezogene Daten für Unbefugte: Verwenden Sie benutzerbezogene und benutzerdefinierte Anmeldeinformationen. Standard für das Setzen von Passwörtern (z. B. Sonderzeichen, Mindestlänge, regelmäßiger Passwortwechsel) Verbot der Passwortfreigabe Berechtigungskonzept auf Anwendungs- und Datenebene mit differenzierten Berechtigungsstufen (Profile, Rollen, Transaktionen und Objekte) Protokollierung der vergebenen Zugriffsberechtigungen Verwendung von Signaturen und Zertifikaten zur Sicherstellung der Autorschaft und Berechtigung zum Wissen. Verschlüsselung von Daten und Datenträgern je nach Schutzbedarf. Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken nach Schutzklassenkonzept Verbot der Nutzung privater Datenträger Richtlinie zum Kopieren von Daten. Zugriffsschutz durch Bildschirmschoner</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Access 2: Measures to prevent access to data processing equipment for unauthorized persons: Determination of persons entitled to enter. Access control devices using personalized and coded ID cards with photo. Access regulation for non-businesspersons. Setting up different security zones with different access authorizations Documentation of the granting and withdrawal of access authorizations Burglary alarm system with alarm transmission to the continuously manned security control center or to the police Additional access control measures as well as door condition monitoring for server rooms Escape door monitoring Restrictive key rules Visitor stays only in the company of employees of the Contractor.</p>	<p>Zugang 2: Maßnahmen zur Verhinderung des Zugangs zu Datenverarbeitungsanlagen für Unbefugte: Ermittlung der einreiseberechtigten Personen. Zugangskontrollgeräte mit personalisierten und codierten ID-Karten mit Foto. Zugangsregelung für Nichtkaufleute. Einrichtung verschiedener Sicherheitszonen mit unterschiedlichen Zutrittsberechtigungen Dokumentation der Erteilung und Entziehung von Zutrittsberechtigungen Einbruchmeldeanlage mit Alarmweiterleitung an die durchgehend besetzte Sicherheitsleitstelle oder an die Polizei Zusätzliche Zutrittskontrollmaßnahmen sowie Türzustandsüberwachung für Serverräume Fluchttürüberwachung Restriktive Schlüsselregeln Der Besucher hält sich nur in Begleitung von Mitarbeitern des Auftragnehmers auf.</p>

<p>Obligation to carry an identity card. Video recording in specific areas Video surveillance of the entrances Biometric access locks (e.g. to server rooms)</p>	<p>Pflicht zum Mitführen eines Personalausweises. Videoaufnahmen in bestimmten Bereichen Videoüberwachung der Eingänge Biometrische Zugangsschleusen (z. B. zu Serverräumen)</p>
<p>Access control to data processing systems Measures to prevent data processing systems from being used by unauthorized persons: Password procedures (including specifications regarding the use of special characters, minimum length, regular password change) Bios Passwords Prohibition of password sharing Automatic screen locking in case of inactivity by time. Locking workstations and/or usernames in case of multiple failed access attempts Regular access eligibility checks Logging the use of access permissions Foreclosure of internal networks by setting up firewall systems. Encryption of data and hard drives according to the protection class concept Housing locks</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Zugangskontrolle zu Datenverarbeitungsanlagen Maßnahmen gegen die Nutzung von Datenverarbeitungsanlagen durch Unbefugte: Passwortverfahren (inkl. Vorgaben zur Verwendung von Sonderzeichen, Mindestlänge, regelmäßiger Passwortwechsel) Bios-Passwörter Verbot der Passwortfreigabe Automatische Bildschirmsperre bei Inaktivität nach Zeit. Sperrungen von Workstations und/oder Benutzernamen bei mehreren fehlgeschlagenen Zugriffsversuchen Regelmäßige Zugangsberechtigungsprüfungen Protokollierung der Nutzung von Zugriffsberechtigungen Abschottung interner Netzwerke durch Einrichtung von Firewall-Systemen. Verschlüsselung von Daten und Festplatten nach dem Schutzklassenkonzept Gehäuseschlösser</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Transfer control Measures to prevent unauthorized knowledge, traceability and integrity in data transmission: Encryption of data and data carriers depending on their need for protection, in particular by means of file and hard drive encryption on a hardware or software basis (e.g. Secude Secure File, SecureDoc Disk Encryption, Truecrypt) Encryption of the transmission of data, especially when transmitted over public networks (e.g. ssl, tls) Using Virtual Private Networks (VPN) Use of lockable transport containers. Data protection-compliant destruction of data, data carriers and printouts according to protection class concept Electronic signature Careful selection of transport personnel</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Transferkontrolle Maßnahmen zur Verhinderung unbefugter Kenntnisnahme, Rückverfolgbarkeit und Integrität bei der Datenübertragung: Verschlüsselung von Daten und Datenträgern je nach Schutzbedürfnis, insbesondere mittels Datei- und Festplattenverschlüsselung auf Hard- oder Softwarebasis (z.B. Secude Secure File, SecureDoc Disk Encryption, Truecrypt) Verschlüsselung der Datenübertragung, insbesondere bei der Übertragung über öffentliche Netze (z.B. ssl, tls) Verwenden von virtuellen privaten Netzwerken (VPN) Verwendung von abschließbaren Transportbehältern. Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken nach Schutzklassenkonzept Elektronische Unterschrift Sorgfältige Auswahl des Transportpersonals</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Order control (when subcontractors are used) Measures to ensure that personal data processed on behalf of the order are processed only under the direction of the Client: criteria for the selection of Contractors (references, certifications, quality labels) Detailed written regulations (contract/agreement) of the contract relationships and formalization of the entire order process, including the use of subcontractors, clear rules of responsibilities and responsibilities. Ensuring that the execution of the order is controlled and documented.</p>	<p>Auftragssteuerung (bei Einsatz von Subunternehmern) Maßnahmen, um sicherzustellen, dass die im Auftrag verarbeiteten personenbezogenen Daten nur auf Weisung des Auftraggebers verarbeitet werden: Kriterien für die Auswahl von Auftragnehmern (Referenzen, Zertifizierungen, Gütesiegel) Detaillierte schriftliche Regelungen (Vertrag/Vereinbarung) der Vertragsverhältnisse und Formalisierung des gesamten Bestellprozesses, einschließlich des Einsatzes von Subunternehmern, klare Verantwortlichkeiten und Verantwortlichkeiten. Sicherstellen, dass die Ausführung des Auftrags kontrolliert und dokumentiert wird.</p>

<p>Agreement of contractual penalties (with subcontractors) for breaches of instructions given. Contractual agreement with subcontractors to oblige own and external employees to keep data secret.</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Vereinbarung von Vertragsstrafen (mit Subunternehmern) bei Verstößen gegen erteilte Weisungen. Vertragliche Vereinbarung mit Subunternehmern, eigene und externe Mitarbeiter zur Geheimhaltung von Daten zu verpflichten.</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>
<p>Separation control Separation control measures: Logical or technical separation of data User profiles / separation of user accounts Different access permissions Storage in specific storage areas Separation of processing systems</p> <p>Comment: These measures are mainly fulfilled by our service provider, Microsoft Azure.</p>	<p>Trennkontrolle Maßnahmen zur Trennungskontrolle: Logische oder technische Trennung von Daten Benutzerprofile / Trennung von Benutzerkonten Unterschiedliche Zugriffsberechtigungen Lagerung in bestimmten Lagerbereichen Trennung von Verarbeitungssystemen</p> <p>Anmerkung: Diese Maßnahmen werden hauptsächlich von unserem Dienstleister Microsoft Azure erfüllt.</p>

ANHANG 3: LISTE DER UNTERAUFTRAGSVERARBEITER

Name and location of the subprocessor / Name und Standort des Unterauftragsverarbeiters	Brief description of the service performed by the sub-processor/ Kurze Beschreibung der vom Unterauftragsverarbeiter erbrachten Leistung
Microsoft Azure Europe (Germany or in another EU Country)	Deployment of IaaS and PaaS Azure Infrastructures for the deployment of iGrafX SaaS applications and data storage Bereitstellung von IaaS und PaaS Azure Infrastrukturen zur Bereitstellung von iGrafX SaaS-Anwendungen und Datenspeicherung
iGrafX, LLC 8100 SW Nyberg St., Suite 450 Tualatin, OR 97062 USA	Support Incident and Change Management Ticket System, Resource and Operations Management, Availability Management, Release and Distribution Management Support Incident- und Change Management Ticketsystem, Ressourcen- und Betriebsmanagement, Verfügbarkeitsmanagement, Release- und Distributionsmanagement
Atlassian 350 Bush Street Floor 13 San Francisco, CA 94104 USA	Jira for support ticket/help desk management. Jira für die Verwaltung von Support-Tickets/Helpdesk.
Mailgun dba Sinch Email, a unit of Sinch America, Inc. 112 E Pecan St, #1135 San Antonio, TX, 78205 USA	Cloud-based email notification services. Cloud-basierte E-Mail-Benachrichtigungsdienste.