DATENVERARBEITUNGSVEREINBARUNG

Diese Datenverarbeitungsvereinbarung („DVV“) ist die Vereinbarung der Parteien in Bezug auf die Verarbeitung personenbezogener Daten und ergänzt alle Lizenz-, Abonnement-, Dienst- oder sonstigen schriftlichen oder elektronischen Verträge (die „**Verträge**“) zwischen Trimble und dem Kunden für den Erwerb von Diensten (einschließlich Software-as-a-Service [Saas], deren zugehörige Trimble Offline-Anwendungen oder mobile Anwendungen und Support – und im Vertrag oder im Folgenden als „Dienste“ oder anderweitig definiert), in deren Verlauf Trimble personenbezogene Daten vom Kunden erhält.

Der Kunde schließt diese DVV ab, (i) indem er den Vertrag unterzeichnet oder anderweitig akzeptiert, (ii) indem er sie im eigenen Namen und gemäß den geltenden Datenschutzgesetzen und -vorschriften im Namen und im Auftrag von autorisierten verbundenen Unternehmen unterzeichnet, wenn und soweit Trimble personenbezogene Daten verarbeitet. Nur für die Zwecke dieser DVV und sofern nicht anders angegeben, umfasst der Begriff „Kunde“ den Kunden und die autorisierten verbundenen Unternehmen.

In Verbindung mit der Erbringung der Dienste für den Kunden laut Vertrag kann Trimble personenbezogene Daten im Namen des Kunden verarbeiten. Die Parteien vereinbaren, die folgenden Bestimmungen in Bezug auf personenbezogene Daten einzuhalten.

RECHTMÄSSIGER ABSCHLUSS DIESER DVV:

I. Diese DVV setzt sich aus dem DVV-Hauptteil und den Anhängen 1 bis 3 zusammen.
II. Sie wurde im Namen von Trimble vorunterzeichnet. Die Standardvertragsklauseln (wie weiter unten definiert) sind zur Bezugnahme beigefügt.
III. Wenn der Kunde diese DVV ausfüllen und abschließen möchte, muss er wie folgt vorgehen:
    a. Füllen Sie das Unterschriftsfeld aus und unterschreiben Sie auf Seite 6.
    b. Füllen Sie die Informationen als Datenexporteur auf Seite 6.
IV. Senden Sie die ausgefüllte und unterzeichnete DVV unter Angabe der Kundennummer Ihres Unternehmens (wie auf der entsprechenden Rechnung von Trimble angegeben) per E-Mail an privacy@trimble.com an Trimble.

GELTUNGSBEREICH DIESER DVV:

- Wenn der Kunde, der diese DVV akzeptiert, einen entsprechenden Vertrag abgeschlossen hat, ist diese DVV ein Zusatz zu diesem Vertrag und bildet einen Teil davon, und die Trimble-Organisation, die diesbezüglich Vertragspartei ist, ist zugleich Vertragspartei dieser DVV.
- Wenn der Kunde, der diese DVV unterzeichnet, eine Bestellung aufgegeben hat, die von Trimble oder einem seiner verbundenen Unternehmen angenommen wurde, aber selbst keine Vertragspartei des diesbezüglichen Vertrags ist, stellt diese DVV einen Zusatz zu dieser Bestellung (einschließlich etwaiger Verlängerungsbestellungen) dar, und die Trimble-Organisation, bei der diese Bestellung aufgegeben wurde, ist Vertragspartei dieser DVV.
- Wenn der Kunde, der die DVV unterzeichnet, Trimble-Dienste über einen autorisierten Vertriebspartner von Trimble erworben hat, muss der Kunde dies auf Seite 6 angeben und eine von Trimble oder dem Vertriebspartner ausgestellte Kundennummer bereitstellen, oder, falls diese fehlt, eine Bestätigung des Vertriebspartners darüber bereitstellen, dass der Kunde einen Trimble-Dienst abonniert hat. In diesem Fall gilt diese DVV als direkter Vertrag zwischen dem Kunden und Trimble.
- Wenn die juristische oder natürliche Person, die diese DVV unterzeichnet, weder verbindlich an einer Bestellung noch an einem Vertrag beteiligt ist und kein indirekter Kunde über einen Vertriebspartner ist, ist diese DVV nicht gültig und nicht rechtsverbindlich. Die betreffende juristische oder natürliche Person sollte verlangen, dass die mit ihr verbundene Vertragspartei des diesbezüglichen Vertrags, diese DVV unterzeichnet oder schriftlich beantragt, selbst Vertragspartei zu werden.

Diese DVV ersetzt keine vergleichbaren oder zusätzlichen Rechte in Bezug auf die Verarbeitung von Kundendaten, die im Vertrag enthalten sind (einschließlich aller bestehenden Datenverarbeitungszusätze zum Vertrag).

DATENVERARBEITUNGSBEDINGUNGEN

1. DEFINITIONEN

„**Verbundenes Unternehmen**“ bezieht sich auf die Organisation, die das vertragschließende Unternehmen direkt oder indirekt kontrolliert, von ihm kontrolliert wird oder mit ihm unter gemeinsamer Kontrolle steht. „Kontrolle“ im Sinne dieser Definition bedeutet direktes oder indirektes Eigentum oder Kontrolle von mehr als 50 % der ausstehenden stimmberechtigten Anteile des vertragschließenden Unternehmens.

„**Autorisiertes verbundenes Unternehmen**“ bezieht sich auf ein oder mehrere verbundene Unternehmen des Kunden, die (i) einem oder mehreren Datenschutzgesetzen unterliegen und (ii) gemäß dem Vertrag zwischen dem Kunden und Trimble zur Nutzung der Dienste berechtigt sind, aber keine eigene Bestellung bei Trimble vereinbart in Auftrag gegeben haben und keine „Kunden“ im Sinne des Vertrags sind.

„**CCPA**“ ist der California Consumer Privacy Act, Cal. Civ. Code § 1798.100 ff. und seine Durchführungsbestimmungen.

„**Datenverantwortlicher**“ ist die Stelle, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt.

„**Kunde**“ bezieht sich auf die juristische oder natürliche Person, die den Vertrag abgeschlossen hat, zusammen mit den verbundenen Unternehmen (solange sie verbundene Unternehmen bleiben), die Bestellformulare unterzeichnet haben.

„**Kundendaten**“ bezieht sich auf die im Vertrag als „Kundendaten“ oder „Ihre Daten“ definierten Inhalte.

„**Datenschutzgesetze und -vorschriften**“ sind alle Gesetze und Vorschriften, einschließlich der Gesetze und Vorschriften der Europäischen Union, des Europäischen Wirtschaftsraums und ihrer Mitgliedstaaten, der Schweiz und des United Kingdom, der in Anhang 3 aufgeführten Länder und aller anderen Länder, in denen der Kunde oder ein mit dem Kunden verbundenes Unternehmen einen Sitz hat, soweit sie auf die Verarbeitung personenbezogener Daten im Rahmen des Vertrags anwendbar sind.

„**Datensubjekt**“ (auch Betroffener) ist die Person, auf die sich die personenbezogenen Daten beziehen.

„**Europa**“ steht für die Europäische Union (EU), den Europäischen Wirtschaftsraum (EWR) und die Schweiz.

„**DSGVO**“ bezieht sich auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Europäischen Rates.

„**Personenbezogene Daten**“ sind alle Informationen, die sich auf (i) eine identifizierte oder identifizierbare natürliche Person und (ii) eine identifizierte oder identifizierbare juristische Person beziehen (wobei diese Informationen nach den geltenden Datenschutzgesetzen und -vorschriften in ähnlicher Weise wie personenbezogene Daten oder persönlich identifizierbare Informationen geschützt sind), sofern es sich bei diesen Daten um Kundendaten handelt.

„**Verarbeitung**“ bezieht sich auf jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Abfolge von Vorgängen im Zusammenhang mit personenbezogenen Daten, beispielsweise das Erheben, das Erfassen, die Organisation, die Strukturierung, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Sperren, das Löschen oder die Vernichtung.

„**Auftragsverarbeiter**“ bezeichnet die Stelle, die personenbezogene Daten auf Anweisung und im Namen des Datenverantwortlichen verarbeitet, gegebenenfalls einschließlich eines „Dienstanbieters“, wie dieser Begriff im CCPA definiert ist.

„**Öffentliche Behörde**“ steht für Regierungsbehörden oder Strafverfolgungsbehörden, einschließlich Justizbehörden.

„**EU-Standardvertragsklauseln**“ bezieht sich auf einen Vertrag, der entweder (i) zwischen einem verbundenen Unternehmen von Trimble und Trimble Inc. oder (ii) zwischen dem Kunden und Trimble Inc. abgeschlossen wird, jeweils gemäß dem Durchführungsbeschluss (EU) 2021/914.

„**Unterauftragsverarbeiter**“ bezeichnet jeden von Trimble oder einem Mitglied der Trimble-Gruppe beauftragten Auftragsverarbeiter.

„**Trimble**“ bezeichnet je nach Fall die Trimble-Organisation, die eine Vertragspartei dieser DVV ist, wie oben im Abschnitt „GELTUNGSBEREICH DIESER DVV“ angegeben. Als Auftragsverarbeiter handelnde Trimble-Organisationen sind: Trimble Inc. ein Unternehmen mit Sitz in Delaware, Trimble Europe B.V. ein Unternehmen mit Sitz in den Niederlanden, Trimble International B.V, ein in den Niederlanden eingetragenes Unternehmen, Trimble UK Ltd, ein in England und Wales eingetragenes Unternehmen, Trimble Maps, Ltd, ein in England und Wales eingetragenes Unternehmen, Trimble Technologies Ireland Ltd, ein in Irland eingetragenes Unternehmen, Trimble France SAS, ein in Frankreich eingetragenes Unternehmen, Trimble Solutions Sandvika AS, ein in Norwegen eingetragenes Unternehmen, Trimble Finland Corporation, ein in Finnland eingetragenes Unternehmen, Trimble Forestry Europe Corporation, ein in Finnland eingetragenes Unternehmen, Lakefield eTechnologies Ltd, ein in Irland eingetragenes Unternehmen, Trimble GmbH, ein in Deutschland eingetragenes Unternehmen, bzw. Trimble Germany GmbH, ein in Deutschland eingetragenes Unternehmen.

„**Trimble-Gruppe**“ bezeichnet Trimble und seine mit der Verarbeitung personenbezogener Daten befassten verbundenen Unternehmen.

2. VERARBEITUNG VON PERSONENBEZOGENEN DATEN

2.1 Rollen der Parteien: Die Parteien der Vereinbarung erkennen an und vereinbaren, dass in Bezug auf die Verarbeitung personenbezogener Daten der Kunde der Datenverantwortliche ist, Trimble ein Auftragsverarbeiter ist, und dass Trimble oder Mitglieder der Trimble-Gruppe Unterauftragsverarbeiter gemäß den Anforderungen im nachstehenden Abschnitt beauftragen, vorausgesetzt, dass Trimble der Datenverantwortliche für die Verarbeitung von Kundenkontodaten ist.

2.2 Verarbeitung von personenbezogenen Daten durch den Kunden: Der Kunde muss bei der Nutzung der Dienste personenbezogene Daten in Übereinstimmung mit den Anforderungen der Datenschutzgesetze und -vorschriften verarbeiten. Um Zweifel auszuschließen, müssen die Vorgaben des Kunden für die Verarbeitung personenbezogener Daten die Datenschutzgesetze und -vorschriften erfüllen. Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten sowie für die Mittel, mit denen der Kunde die personenbezogenen Daten erworben hat. Trimble wird den Kunden unverzüglich informieren, wenn eine Vorgabe aus seiner Sicht gegen Datenschutzgesetze und -vorschriften oder gegen andere gesetzliche Bestimmungen verstößt.

2.3 Verarbeitung von personenbezogenen Daten durch Trimble: Trimble verarbeitet personenbezogene Daten nur im Auftrag und in Übereinstimmung mit den Vorgaben des Kunden, auch im Hinblick auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Der Kunde weist Trimble an, personenbezogene Daten für die folgenden Zwecke zu verarbeiten: (i) Verarbeitung in Übereinstimmung mit dem Vertrag und den relevanten Bestellungen; (ii) Verarbeitung, die von den Benutzern bei der Nutzung der Dienste veranlasst wird; (iii) Verarbeitung zur Erfüllung anderer angemessener Vorgaben des Kunden, sofern diese Vorgaben mit den Bedingungen des Vertrags übereinstimmen; und (iv) Verarbeitung zum Zweck der Anonymisierung in Übereinstimmung mit den Datenverwendungsklauseln im Vertrag (und in Anhang 1 enthalten).

TRIMBLE HANDELT NICHT ALS AUFTRAGSVERARBEITER FÜR FOLGENDE PERSONENBEZOGENE DATEN: Anmelde- und Kontaktdaten der Benutzer, Daten über die Nutzung der Software und durch Sicherheitsmaßnahmen erzeugte Daten („**Kundenkontodaten**)“.

2.4 Umfang und Zweck sowie Kategorien von personenbezogenen Daten und Datensubjekten: Der Gegenstand der Verarbeitung personenbezogener Daten durch Trimble ist die Erbringung der Dienste gemäß dem Vertrag. Die Arten von personenbezogenen Daten und die Kategorien der Datensubjekte, die im Rahmen dieser DVV verarbeitet werden, sind in Anhang 1 (Beschreibung der Verarbeitung) dieser DVV näher beschrieben.

3. RECHTE VON DATENSUBJEKTEN

3.1 Rechte von Datensubjekten: Unter Berücksichtigung der Art der Verarbeitung unterstützt Trimble den Kunden durch die Bereitstellung geeigneter technischer und organisatorischer Maßnahmen, soweit dies möglich ist, um die Verpflichtung des Kunden zu erfüllen, auf Anfragen von Datensubjekte zur Ausübung ihrer Rechte gemäß den Datenschutzgesetzen und -vorschriften zu reagieren. Soweit der Kunde bei der Nutzung der Dienste nicht in der Lage ist, diese Rechte selbst auszuüben, wird Trimble jedem wirtschaftlich angemessenen Ersuchen des Kunden nachkommen, solche Handlungen zu erleichtern, soweit Trimble gesetzlich dazu befugt ist. Soweit dies rechtlich zulässig ist, trägt der Kunde die Kosten, die durch eine solche Unterstützung durch Trimble entstehen.

3.2 Direkte Anfragen eines Datensubjekts: Trimble wird im gesetzlich zulässigen Rahmen den Kunden unverzüglich benachrichtigen, wenn eine Anfrage eines Datensubjekts zur Ausübung seiner entsprechenden Rechte gemäß Abschnitt 3.1 eingeht. Trimble wird auf eine solche Anfrage eines Datensubjekts nicht ohne vorherige Zustimmung des Kunden in Textform antworten, außer um zu bestätigen, dass sich die Anfrage auf den Kunden bezieht, womit der Kunde hiermit einverstanden ist.

4. TRIMBLE-MITARBEITER MIT KUNDENBEZUG

4.1 Allgemeines: Trimble und der Kunde ergreifen Maßnahmen, um sicherzustellen, dass jede natürliche Person, die unter ihrer jeweiligen Autorität handelt und Zugang zu Kundendaten hat, keine Kundendaten verarbeitet, es sei denn, sie ist aufgrund von Datenschutzgesetzen und -vorschriften dazu verpflichtet.

4.2 Vertraulichkeit: Trimble stellt sicher, dass Trimble-Mitarbeiter, die mit der Verarbeitung personenbezogener Daten befasst sind, über die Vertraulichkeit der personenbezogenen Daten informiert sind, eine angemessene Schulung zu ihren Verantwortlichkeiten erhalten haben und eine schriftliche Geheimhaltungsvereinbarung unterschrieben haben. Trimble stellt sicher, dass die Gültigkeit solcher Geheimhaltungsvereinbarungen auch nach Beendigung des Arbeitsverhältnisses fortbesteht.

4.3 Zuverlässigkeit: Trimble ergreift wirtschaftlich angemessene Maßnahmen, um die Zuverlässigkeit der mit der Verarbeitung personenbezogener Daten befassten Trimble-Mitarbeiter zu gewährleisten.

4.4 Beschränkung des Datenzugriffs: Trimble stellt sicher, dass der Zugriff von Mitarbeitern auf personenbezogene Daten auf diejenigen Mitarbeiter beschränkt ist, die Dienste in Übereinstimmung mit dem Vertrag erbringen.

5. UNTERAUFTRAGSVERARBEITER

5.1 Beauftragung von Unterauftragsverarbeitern: Der Kunde bestätigt und erklärt sich damit einverstanden, dass (i) die verbundenen Unternehmen von Trimble als Unterauftragsverarbeiter eingesetzt werden können und (ii) Trimble bzw. die verbundenen Unternehmen von Trimble im Zusammenhang mit der Erbringung der Dienste Unterauftragsverarbeiter von Dritten einsetzen können. In diesem Fall müssen Trimble und die verbundenen Unternehmen von Trimble jedem Unterauftragsverarbeiter durch einen Vertrag oder einen anderen Rechtsakt dem Wesen nach ähnliche Datenschutzverpflichtungen auferlegen, wie sie in dieser DVV vorgesehen sind. Der Vertrag oder anderweitige Rechtsakt muss ausreichende Garantien dafür enthalten, dass der Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen dafür ergreift, dass die Verarbeitung der Daten die Anforderungen der Datenschutzgesetze und -vorschriften erfüllt.

5.2 Liste der derzeitigen Unterauftragsverarbeiter und Meldung neuer Unterauftragsverarbeiter. Die aktuelle Liste der Unterauftragsverarbeiter, die mit der Verarbeitung personenbezogener Daten für die Erbringung der einzelnen Dienste beauftragt sind, einschließlich einer Beschreibung ihrer Verarbeitungstätigkeiten und der Länder, in denen sie ansässig sind, ist bei https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center unter „Additional Resources“ („Sub-processor Lists“) einsehbar. Der Kunde erteilt hiermit seine Zustimmung zu diesen Unterauftragsverarbeitern, deren Standorten und Verarbeitungstätigkeiten in Bezug auf seine personenbezogenen Daten und weist Trimble entsprechend an. Trimble informiert über Änderungen bei den Unterauftragsverarbeitern in seinen Versionshinweisen, Kunden-Updates oder ähnlichen Mitteilungen, die als Mitteilung im Sinne von Abschnitt [9.2 der EU-Standardvertragsklauseln] gelten.

5.3 Widerspruchsrecht für neue Unterauftragsverarbeiter: Um von seinem Recht Gebrauch zu machen, dem Einsatz eines neuen Unterauftragsverarbeiters durch Trimble zu widersprechen, muss der Kunde Trimble unverzüglich in Textform an privacy@trimble.com innerhalb von dreißig (30) Werktagen nach Erhalt der Mitteilung von Trimble gemäß dem in Abschnitt 5.2 dargelegten Mechanismus informieren. Falls der Kunde einem neuen Unterauftragsverarbeiter widerspricht und dieser Widerspruch nicht unangemessen ist, unternimmt Trimble angemessene Anstrengungen, um dem Kunden eine Änderung der Dienste zur Verfügung zu stellen oder eine wirtschaftlich angemessene Änderung der Konfiguration oder Nutzung der Dienste durch den Kunden zu empfehlen, um die Verarbeitung personenbezogener Daten durch den widersprochenen neuen Unterauftragsverarbeiter zu vermeiden, ohne den Kunden unangemessen zu belasten. Ist Trimble nicht in der Lage, eine solche Änderung innerhalb einer angemessenen Frist bereitzustellen, die sechzig (60) Tage nicht überschreiten darf, kann der Kunde die betreffenden Bestellungen und Verträge nur in Bezug auf die Dienste kündigen, die von Trimble nicht ohne den beanstandeten neuen Unterauftragsverarbeiter erbracht werden können, indem er Trimble schriftlich davon in Kenntnis setzt. Trimble erstattet dem Kunden alle im Voraus bezahlten Gebühren für die verbleibende Laufzeit der Bestellungen nach dem Datum des Inkrafttretens der Kündigung in Bezug auf die gekündigten Dienste.

5.4 Haftung: Trimble haftet für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter in demselben Umfang, in dem Trimble haften würde, wenn die Dienste jedes Unterauftragsverarbeiters direkt gemäß den Bedingungen dieser DVV erbracht würden, sofern im Vertrag nichts anderes festgelegt ist.

6. SICHERHEIT, AUDITS/PRÜFUNGEN UND UNTERSTÜTZUNG

6.1 Sicherheit der Verarbeitung. Trimble unterhält administrative, physische und technische Schutzmaßnahmen zum Schutz der Sicherheit, Vertraulichkeit und Integrität von Kundendaten, einschließlich personenbezogener Daten, wie in Anhang 1 dargelegt. Trimble überwacht regelmäßig die Einhaltung dieser Sicherheitsvorkehrungen. Trimble wird die Gesamtsicherheit der Dienste während der Vertragslaufzeit nicht wesentlich verringern.

6.2 Audits: Trimble führt von Zeit zu Zeit Audits und Prüfungen durch (sofern angemessen, auch Audits durch externe Prüfer), um die Einhaltung der Datenschutzgesetze und dieser DVV sowie (soweit angemessen) der Branchenstandards wie ISO 27001 zu gewährleisten.Trimble stellt dem Kunden auf Anfrage alle erforderlichen Informationen zur Verfügung (auch entsprechende Auditberichte), um die Einhaltung seiner Verpflichtungen aus den geltenden Datenschutzgesetzen und dieser DVV nachzuweisen. Je nach den angeforderten Informationen kann Trimble vom Kunden die Unterzeichnung einer Vertraulichkeitsvereinbarung (NDA) verlangen.

6.3 Unterstützung des Kunden: Trimble unterstützt den Kunden bei der Einhaltung der Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Benachrichtigung und Mitteilung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzungen und vorherige Konsultationen mit der Aufsichtsbehörde gemäß den Datenschutzgesetzen und -vorschriften.

6.4 Handhabung von Sicherheitsverletzungen und Benachrichtigungen: Im Falle einer Verletzung des Schutzes personenbezogener Daten gemäß den Datenschutzgesetzen und -bestimmungen sieht Trimble Richtlinien und Verfahren für die Handhabung von Sicherheitsvorfällen vor und benachrichtigt den Kunden im gesetzlich zulässigen Rahmen unverzüglich über eine solche Verletzung.

7. RÜCKGABE UND LÖSCHUNG VON KUNDENDATEN

Trimble wird nach Beendigung der Erbringung der Dienste nach Wahl des Kunden die Kundendaten an den Kunden zurückgeben und/oder die Kundendaten gemäß den im Vertrag oder der Dienstbeschreibung angegebenen Verfahren und Fristen löschen, es sei denn, die Gesetze, denen der Kunden untersteht, schreiben die Speicherung von Kundendaten vor.

8. ZUGRIFFSANFRAGEN DURCH BEHÖRDEN

8.1 Sofern dies nicht durch geltendes Recht untersagt ist, informiert Trimble den Kunden in allgemeiner Form über Anfragen, Anordnungen oder ähnliche Aufforderungen eines Gerichts, einer zuständigen Behörde, einer Strafverfolgungsbehörde oder einer anderen staatlichen Stelle („Anfragen von Strafverfolgungsbehörden“), die sich auf die Verarbeitung personenbezogener Daten gemäß diesen Klauseln beziehen.

8.2 Trimble wird gegen alle Anfragen von Strafverfolgungsbehörden Einspruch erheben und diese mit Rechtsmitteln anfechten, soweit diese unter den gegebenen Umständen angemessen sind. Sollte Trimble aufgrund eines Ersuchens von Strafverfolgungsbehörden gezwungen sein, die gemäß diesen Klauseln übermittelten personenbezogenen Daten offenzulegen, wird Trimble den Kunden in angemessener Weise darüber informieren, um ihm die Möglichkeit zu geben, eine einstweilige Verfügung oder ein anderes geeignetes Rechtsmittel zu beantragen, sofern dies Trimble nicht gesetzlich untersagt ist.

8.3 Falls Trimble personenbezogene Daten an Unterauftragsverarbeiter weitergibt, wählt Trimble Unterauftragsverarbeiter in einem Land außerhalb des Europäischen Wirtschaftsraums aus, das nicht einer Angemessenheitsfeststellung der EU-Kommission unterliegt, und zwar nur nach einer sorgfältigen Prüfung, die (i) eine Überprüfung der vom Unterauftragsverarbeiter zur Verfügung gestellten Transparenzberichte und (ii) eine Bewertung des Übertragungsrisikos umfasst.

9. AUTORISIERTE VERBUNDENE UNTERNEHMEN

9.1 Vertragsverhältnis: Der Kunde unterzeichnet die DVV im eigenen Namen und ggf. im Namen und im Auftrag von autorisierten verbundenen Unternehmen, wodurch eine separate DVV zwischen Trimble und jedem dieser autorisierten verbundenen Unternehmen zustande kommt. Jedes autorisierte verbundene Unternehmen ist an die Verpflichtungen dieser DVV gebunden. Zur Klarstellung: Ein autorisiertes verbundenes Unternehmen ist nicht Vertragspartei und wird auch nicht Vertragspartei, sondern ist lediglich Partei der DVV. Jeder Zugang zu den Diensten und deren Nutzung durch autorisierte verbundene Unternehmen muss den Bedingungen des Vertrags entsprechen, und jede Verletzung der Bedingungen des Vertrags durch ein autorisiertes verbundenes Unternehmen gilt als Verletzung durch den Kunden.

9.2 Kommunikation: Der Kunde als Vertragspartner bleibt für die Koordinierung der gesamten Kommunikation mit Trimble im Rahmen dieser DVV verantwortlich und ist berechtigt, jegliche Kommunikation im Zusammenhang mit dieser DVV im Namen seiner autorisierten verbundenen Unternehmen zu tätigen und zu empfangen.

9.3 Rechte autorisierter verbundener Unternehmen: Wenn ein autorisiertes verbundenes Unternehmen Partei der DVV mit Trimble wird, ist es in dem nach den geltenden Datenschutzgesetzen und -vorschriften erforderlichen Umfang berechtigt, die Rechte gemäß dieser DVV auszuüben und Rechtsmittel einzulegen. Wenn Datenschutzgesetze und -vorschriften verlangen, dass das autorisierte verbundene Unternehmen ein Recht ausübt oder Rechtsmittel gemäß dieser DVV als Datenverantwortlicher einlegt, bevollmächtigt das autorisierte verbundene Unternehmen hiermit den Kunden zur Ausübung solcher Rechte anstelle des autorisierten verbundenen Unternehmens. Darüber hinaus übt der Kunde, der Vertragspartner ist, diese Rechte im Rahmen dieser DVV nicht für jedes autorisierte verbundene Unternehmen einzeln, sondern für alle seine autorisierten verbundenen Unternehmen zusammen aus.

10. Haftungsbegrenzung

Die Haftung jeder Partei und der jeweiligen verbundenen Unternehmen aus oder im Zusammenhang mit dieser DVV und allen DVVs zwischen autorisierten verbundenen Unternehmen und Trimble, ob aus Verletzung einer Vertragsbestimmung, unerlaubter Handlung oder einem anderen Rechtsgrund, unterliegt dem Abschnitt „Haftungsbeschränkung“ des Vertrags, und jede Bezugnahme in diesem Abschnitt auf die Haftung einer Partei bedeutet die Gesamthaftung dieser Partei und ihrer verbundenen Unternehmen aus dem Vertrag und allen DVVs zusammen. Um Zweifel auszuschließen, gilt die Gesamthaftung von Trimble und seinen verbundenen Unternehmen für alle Rechtsansprüche des Kunden und seiner autorisierten verbundenen Unternehmen, die sich aus dem Vertrag und jeder DVV ergeben oder damit in Zusammenhang stehen, für alle Ansprüche sowohl aus dem Vertrag als auch aus allen DVVs, die im Rahmen eines solchen Vertrages festgesetzt wurden, einschließlich der Ansprüche von autorisierten verbundenen Unternehmen. Die Gesamthaftung ist insbesondere nicht so zu verstehen, dass sie für jedes autorisierte verbundene Unternehmen, das eine Vertragspartei einer solchen DVV ist, einzeln und gesamtschuldnerisch gilt. Um weitere Zweifel auszuschließen, gilt jede Bezugnahme auf die DVV in der vorliegenden DVV für diese DVV einschließlich all ihrer Anhänge.

Wenn der Kunde die Dienste über einen Vertriebspartner oder einen anderen Geschäftspartner von Trimble abonniert oder erworben hat, ist die Haftung von Trimble und seinen verbundenen Unternehmen, die sich aus oder im Zusammenhang mit dieser DVV und allen DVVs zwischen autorisierten verbundenen Unternehmen und Trimble ergibt, unabhängig davon, ob es sich um eine Verletzung einer Vertragsbestimmung, eine unerlaubte Handlung oder einen anderen Rechtsgrund handelt, im rechtlich zulässigen Rahmen insgesamt auf den höheren der Beträge beschränkt, die Trimble für diese Dienste erhalten hat, beziehungsweise auf 50.000 EUR.

11. INTERNATIONALE BESTIMMUNGEN

11.1 Grenzüberschreitender Übermittlungsmechanismus: Soweit Trimble personenbezogene Daten verarbeitet, die aus einem der in Anhang 3 (Grenzüberschreitender Übermittlungsmechanismus) dieser DVV aufgeführten juristischen Zuständigkeitsgebiete stammen und dort durch Datenschutzgesetze und -vorschriften geschützt sind, gelten zusätzlich zu den Bestimmungen dieser DVV die in Anhang 3 aufgeführten Bestimmungen in Bezug auf die relevanten Zuständigkeitsgebiete.

11.2 Grenzüberschreitende Datenübermittlungsmechanismen: Soweit die Nutzung der Dienste durch den Kunden einen Weiterleitungsmechanismus erfordert, um Personenbezogene Daten aus einem juristischen Zuständigkeitsgebiet (d. h. dem Europäischen Wirtschaftsraum, dem United Kingdom, der Schweiz, der Türkei oder einem anderen in Anhang 3 (Grenzüberschreitender Übermittlungsmechanismus dieser DVV) aufgeführten Zuständigkeitsgebiet rechtmäßig an Trimble, das sich außerhalb dieses Zuständigkeitsgebiets befindet, zu übermitteln („Übermittlungsmechanismus“), gelten die in Anhang 4 (Grenzüberschreitende Übermittlungsmechanismen) dieser DVV dargelegten Bestimmungen.

12. Verschiedenes

12.1 Konflikte: Im Falle eines Widerspruchs oder einer Unstimmigkeit zwischen den folgenden Dokumenten gilt die folgende Rangfolge: (1) die anwendbaren Bestimmungen in Anhang 4 (Grenzüberschreitender Übermittlungsmechanismus) dieser DVV, (2) die Bestimmungen dieser DVV außerhalb von Anhang 4 (Grenzüberschreitender Übermittlungsmechanismus), (3) der Vertrag.

12.2 Aktualisierungen: Trimble kann die Bedingungen dieser DVV von Zeit zu Zeit aktualisieren, sofern Trimble den Kunden mindestens dreißig (30) Tage im Voraus schriftlich informiert, wenn eine Aktualisierung aufgrund von (a) Änderungen der Datenschutzgesetze und -vorschriften, (b) aufgrund einer Fusion, Übernahme oder einer anderen ähnlichen Transaktion oder (c) aufgrund der Einführung neuer Produkte oder Dienste oder wesentlicher Änderungen an bestehenden Diensten erforderlich ist. Die jeweils aktuellen Bedingungen dieser DVV sind unter trimble.com/privacy einsehbar.

Offizieller Name des Kunden:_____

Adresse

Kundennummer bei Trimble:_____

☐ Der Kunde hat die Dienste über einen autorisierten Vertriebspartner oder Geschäftspartner von Trimble erworben.

Name des Vertriebspartners

Adresse _____

Kundennummer beim Vertriebspartner

☐ Für EU/EWR/UK-Rechnung an Kunden: Der Kunde möchte die EU-Standardvertragsklauseln direkt mit Trimble Inc. abschließen. Wenn dieses Kästchen nicht angekreuzt ist, gilt für die Übermittlung an Trimble Inc. der in Abschnitt 2.2 von Anhang 4 beschriebene Übermittlungsmechanismus oder ein anderer Übermittlungsmechanismus, der zwischen dem verbundenen Trimble-Unternehmen in Europa und Trimble Inc. festgesetzt wurde.

Wenn das obige Kästchen angekreuzt ist: Für den Kunden gelten die folgenden Module als anwendbar:

☐Modul 1/Vertrag 1 ☐ Modul 2/Vertrag 2 ☐ Modul 3/Vertrag 3

☐ Der Kunde entscheidet sich, diese DVV zu unterzeichnen.
Die Unterschriftsberechtigten der Parteien haben diese Vereinbarung ordnungsgemäß unterzeichnet:

KUNDE (unterzeichnet hiermit diese DVV)

Name:

Titel

Datum:

Trimble Inc.

Unterschrift:_____
Name in Druckschrift: Jennifer Allison
Stellenbezeichnung: Senior Vice President und General Counsel
Datum: 15.07.2024

Trimble Europe BV

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble UK Limited

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble France SAS

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble Solutions Sandvika AS

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble Technologies Ireland Limited

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Lakefield eTechnologies Limited

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble International BV

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble Finland Corporation

Unterschrift:_____
Name in Druckschrift: Jürgen Kesper
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble Germany GmbH

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble MAPS Limited.

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble Forestry Europe Corporation

Unterschrift:_____
Name in Druckschrift: RHH Reeder
Stellenbezeichnung: Director
Datum: 15.07.2024

Trimble GmbH

Unterschrift:_____
Name in Druckschrift: Jürgen Kesper
Stellenbezeichnung: Director
Datum: 15.07.2024

Kontaktinformationen für alle Trimble-Organisationen:

privacy@trimble.com

Addressen von Trimble-Organisationen	
Trimble Inc.	**Trimble Europe B.V.**
10368 Westmoor Drive Westminster, CO 80021, USA	Industrieweg 187a 5683CC Best, Niederlande
Trimble UK Limited	**Trimble France SAS**
Trimble House, Gelderd Road, Gildersome, Leeds LS27 7JP Großbritannien	1 Quai Gabriel Péri 94340 Joinville-le-Pont, Frankreich
Trimble Solutions Sandvika AS	**Trimble Technologies Ireland Limited**
Leif Tronstads plass 4 1337 Sandvika, Norwegen	North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Irland
Lakefield eTechnologies Limited	**Trimble International BV**
North Point Business Park, Unit 3d North Point House, New Mallow Rd, Cork, T23 AT2P, Irland	Industrieweg 187a 5683CC Best, Niederlande
Trimble Finland Corporation	**Trimble Germany GmbH**
Hatsinanpuisto 8, 02600 Espoo, Finnland	Am Prime Parc 11, 65479 Raunheim
Trimble MAPS Limited.	**Trimble Forestry Europe Corporation**
53-64 Chancery Lane, Holborn, London England WC2A 1QS Großbritannien	Hatsinanpuisto 8, 02600 Espoo, Finnland
Trimble GmbH	
Am Prime Parc 11, 65479 Raunheim	

ANHANG 1 – BESCHREIBUNG DER VERARBEITUNG

1. KATEGORIEN VON DATENSUBJEKTEN, DEREN PERSONENBEZOGENE DATEN ÜBERMITTELT WERDEN

Der Kunde kann personenbezogene Daten an die Dienste übermitteln, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird und die personenbezogene Daten der folgenden Kategorien von Datensubjekten (betroffenen Personen) enthalten können, aber nicht darauf beschränkt sind:

- Mitarbeiter, leitende Angestellte, Abteilungsleiter, Führungspersonal und Auftragnehmer des Kunden
- Kunden (natürliche Personen) des Kunden, häufig in ihrer Eigenschaft als Empfänger von Lieferungen, Diensten/Dienstleistungen und Produkten
- Mitarbeiter, Vertreter, Berater, freie Mitarbeiter von Kunden des Kunden, Verkäufer und Gegenparteien von Transaktionen, die über die Dienste abgewickelt werden
- Benutzer des Kunden, die vom Kunden zur Nutzung der Dienste autorisiert wurden

2. KATEGORIEN VON ÜBERMITTELTEN PERSONENBEZOGENEN DATEN

Der Kunde kann personenbezogene Daten an die Dienste übermitteln, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird und die die folgenden Kategorien personenbezogener Daten umfassen können, aber nicht darauf beschränkt sind:

- Kontakt- und Stammdaten (Vor- und Nachname, Titel/Stellenbezeichnung, Position)
- Kontaktinformationen (Unternehmen, E-Mail, Telefon, tatsächliche Geschäftsadresse)
- ID-Daten wie Ausweisdaten, Passdaten, Führerscheindaten, IP-Adressen, eindeutige Kennungen (Universal Unique Identifiers, UUID)
- Berufs- und Ausbildungsdaten (Qualifikationen, Erfahrung, Kenntnisse, Fähigkeiten)
- Berufsbezogene Daten (erbrachte Leistungen, Projektbeiträge, zugewiesene Aufträge und Aufgaben, leistungsbezogene Daten, Dienststunden, Ausgaben)
- Standortdaten
- Vertragsbezogene Daten (Abrechnung, Zahlung, Transaktionsverlauf)
- Interaktionsverlauf

3. ÜBERMITTELTE SENSIBLE DATEN (SOFERN ZUTREFFEND)

Übermittlung sensibler Daten (sofern zutreffend) und Anwendung von Beschränkungen oder Schutzvorkehrungen, die der Art der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen, wie z. B. strikte Zweckbindung, Zugangsbeschränkungen (z. B. Datenzugriff nur für Mitarbeiter mit besonderer Schulung), Aufzeichnung des Datenzugriffs, Beschränkungen der Weiterübermittlung oder zusätzliche Sicherheitsmaßnahmen:
Der Datenexporteur kann an die Dienste besondere Datenkategorien übermitteln, deren Umfang vom Datenexporteur nach seinem alleinigen Ermessen bestimmt und kontrolliert wird, und bei denen es sich der Klarheit halber um personenbezogene Daten mit Informationen handelt, aus denen die ethnische Herkunft, politische Ansichten, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, sowie um die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten über das Sexualleben oder die sexuelle Ausrichtung einer natürlichen Person.
Die anwendbaren Sicherheitsmaßnahmen sind weiter unten in Abschnitt 11 von Anhang 2 beschrieben.

4. HÄUFIGKEIT DER ÜBERMITTLUNG

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

Kontinuierliche Übermittlung in Abhängigkeit von der Nutzung der Dienste durch den Kunden.

5. ART DER VERARBEITUNG

Die Art der Verarbeitung bezieht sich auf die Erbringung der Dienste gemäß dem Vertrag.

6. ZWECK VON VERARBEITUNG, DATENÜBERMITTLUNG UND WEITERVERARBEITUNG

Trimble verarbeitet personenbezogene Daten in dem Maße, wie es für die Erbringung der Dienste gemäß dem Vertrag erforderlich ist, wie es in der Dokumentation näher beschrieben ist und wie es der Kunde bei der Nutzung der Dienste vorgibt. Trimble anonymisiert personenbezogene Daten weiter, um Datenanalysen und die Entwicklung von Diensten durchzuführen.

7. DAUER DER VERARBEITUNG

Der Zeitraum, für den die personenbezogenen Daten aufbewahrt werden, oder, falls dies nicht möglich ist, die Kriterien für die Festsetzung dieses Zeitraums:

Trimble verarbeitet personenbezogene Daten wie in der Vereinbarung festgelegt, sofern nichts anderes vereinbart wurde, z. B. in Abschnitt 9 der DVV.

8. ÜBERMITTLUNGEN AN UNTERAUFTRAGSVERARBEITER

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

Der Unterauftragsverarbeiter verarbeitet personenbezogene Daten in dem Maße, wie es für die Erbringung der Dienste gemäß dem Vertrag erforderlich ist. Gemäß Abschnitt 9 dieser DVV verarbeitet der Unterauftragsverarbeiter personenbezogene Daten für die Vertragslaufzeit, sofern nichts anderes schriftlich vereinbart wurde.

Die Identitäten der für die Erbringung der Dienste eingesetzten Unterauftragsverarbeiter und das Land, in dem sie ansässig sind, sind bei trimble.com/privacy unter „Additional Materials“ aufgeführt.

ANHANG 2 – Technische und organisatorische Sicherheitsmaßnahmen

Gegebenenfalls dient dieser Anhang 2 auch als Anhang II zu den EU-Standardvertragsklauseln.

Technische und organisatorische Sicherheitsmaßnahmen

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung von personenbezogenen Daten

Soweit möglich, verschlüsselt Trimble die zwischen Kunden und der Trimble-Anwendung über öffentliche Netzwerke übertragenen Daten mit TLS 1.2 oder höher. Die auf den von Trimble verwalteten Systemen gespeicherten Kundendaten (für AICPA-zertifizierte Produkte – weitere Informationen unter Punkt 7) werden mit AES 256 oder stärkeren Chiffren verschlüsselt.

2. Maßnahmen zur Gewährleistung der kontinuierlichen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste

Trimble verfügt über besondere Cybersicherheit-Mitarbeiter, die für die Überwachung von Sicherheit und Datenschutz zuständig sind. Es wurde zusätzlich zu einem Datenschutzbüro (Office of Data Protection) Führungspersonal für Cybersicherheit und Datenschutz berufen. Außerdem gibt es ein Engineering Leadership Council, das vierteljährlich zusammenkommt, um die Risiken im Bereich Datenschutz und Sicherheit zu erörtern, die innerhalb der Produktportfolios des Sektors gehandhabt werden müssen. Darüber hinaus werden Produktrisiken in einem internen Portal verfolgt. Die Einhaltung der Vorschriften wird monatlich überwacht.

3. Maßnahmen zur Gewährleistung der Fähigkeit, die Verfügbarkeit von personenbezogenen Daten und den Zugriff darauf im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen

Um die Verfügbarkeit von Trimble SaaS-Produkten zu unterstützen, nutzt Trimble branchenführende Cloud-Service-Anbieter (Amazon Web Services / AWS und Microsoft Azure) für die automatische Skalierung, geografisch verteilte Rechenzentren, umfassende Anwendungs- und Infrastrukturüberwachung und Rund-um-die-Uhr-Supportmechanismen.
Trimble unterhält Backups von Datenspeichern, einschließlich Kundendaten, die die Hauptfunktionen der Trimble-Anwendungen unterstützen. Backups werden an einem Ort gespeichert, der nach Möglichkeit geografisch vom primären Datenspeicherort getrennt ist.
Zusätzlich zu den Maßnahmen unserer Dienstanbieter unterhält Trimble eine Funktion zum Reagieren auf Sicherheitsvorfälle, die eine dokumentierte Richtlinie und einen Plan für das Reagieren auf Vorfälle umfasst, um Sicherheitsereignisse und Vorfälle mit Kundendaten zu behandeln. Darin werden Reaktionsprotokolle wie Eindämmung, Beseitigung, Wiederherstellung und Kommunikationsmaßnahmen bei Sicherheitsvorfällen sowie die Rollen und Zuständigkeiten der Trimble-Mitarbeiter und die Verpflichtung zu Nachbesprechungen mit dem Trimble-Management nach einem Vorfall festgelegt.

4. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten

Trimble beauftragt unabhängige Dritte mit der Durchführung regelmäßiger Penetrationstests, einschließlich Sarbanes-Oxley-, PCI-, SOC 1, Typ II-, SOC 2 Typ II-, ISO27001- oder NIST 800-171-äquivalenter Prüfungen auf jährlicher Basis, sofern dies für die Einhaltung von Vorschriften erforderlich ist. Darüber hinaus führt Trimble regelmäßig interne Schwachstellen- und Penetrationstests für die entsprechenden Produkte und Plattformen in Verbindung mit dem Cybersicherheitsprogramm und den Richtlinienanforderungen von Trimble durch. Trimble kann Bewertungen neuer Anbieter oder Partner durchführen, wenn das Geschäftsrisiko eine Überprüfung rechtfertigt. Trimble ermutigt Dritte, alle Cybersicherheitsprobleme, Vorfälle und Schwachstellen im Zusammenhang mit unseren Produkten, Diensten oder Websites zu melden.

5. Maßnahmen zur Identifizierung und Autorisierung der Benutzer

Bei Produkten, die Trimble ID (TID, Trimble Identity) zur Authentifizierung nutzen, sorgt Trimble für eine sichere Kennwortverarbeitung. Darüber hinaus können einige Trimble-Produkte die Integration von Single-Sign-On (SSO) mit einem Kundenidentitätsanbieter unter Verwendung von Security Assertion Markup Language (SAML) und Multi-Faktor-Authentifizierung (MFA) unterstützen.

6. Maßnahmen zum Schutz der Daten bei der Übermittlung

Wie unter Punkt 1 beschrieben, verschlüsselt Trimble Kundendaten, die über öffentliche Netze zwischen Kunden und der Trimble-Anwendung übertragen werden, möglichst stets mit aktuellen Verschlüsselungscodes.

7. Maßnahmen zum Schutz der Daten während der Speicherung

Wie unter Punkt 1 beschrieben, werden die auf dem von Trimble verwalteten Datenspeicher gespeicherten Kundendaten mit AES 256 oder stärker verschlüsselt, wenn die Trimble-Produkte zurzeit nach AICPA SOC 1, Typ II, SOC 2, Typ II oder NIST 800-171 zertifiziert sind. Ausführlichere Informationen finden Sie unter Punkt 11.

8. Maßnahmen zur Gewährleistung der physischen Sicherheit der Standorte, an denen personenbezogene Daten verarbeitet werden

Die SaaS-Produkte, -Anwendungen und -Dienste von Trimble werden in der Regel mit Kundendaten gehostet, die in Rechenzentren von Amazon Web Services (AWS), Microsoft Azure oder Google Cloud Platform (GCP) gespeichert werden. Daher ist Trimble auf die physischen, umweltbezogenen und infrastrukturellen Kontrollen dieser Plattformen angewiesen. Trimble prüft regelmäßig die von diesen Anbietern vorgelegten Zertifizierungen und Bescheinigungen Dritter in Bezug auf die Effektivität der Kontrollen in ihren Rechenzentren.

9. Maßnahmen zur Sicherstellung der Ereignisprotokollierung

Trimble unterhält zahlreiche Protokolle für Cybersicherheits-Tools sowie Protokolle für die Sicherheitsüberprüfung von Anwendungen und Infrastrukturen. Sicherheitsprotokolle werden mit der SIEM-Technologie in Kombination mit Ereigniskorrelation analysiert, um anomale Aktivitäten zu erkennen.

10. Maßnahmen zur Sicherstellung der Systemkonfiguration, einschließlich der Standardkonfiguration

Trimble nutzt gängige Branchenstandards, um die Cybersicherheit durch sichere Konfiguration und Tiefenverteidigung (Defense-in-Depth) zu erhöhen. Trimble wendet Sicherheitspatches auf seine Systeme in Übereinstimmung mit der Trimble Secure Development Lifecycle Policy (TSDLCP) an.

11. Maßnahmen zur Steuerung und Verwaltung der internen IT und der IT-Sicherheit

Für SOC 1, Typ II, SOC 2, Typ II oder NIST 800-171 zertifizierte Produkte von Trimble nutzen Mitarbeiter mit Zugriff auf Kundendaten rollenbasierte und Least-Privilege-Prinzipien zur Zugriffskontrolle. Die Mitarbeiter erhalten nur so viel Zugriff auf Kundendaten, wie für die sichere Erfüllung ihrer Aufgaben erforderlich ist. Der Fernzugriff auf Trimble-Systeme erfordert eine verschlüsselte Kommunikation über gesicherte Protokolle und die Verwendung einer Multi-Faktor-Authentifizierung. Trimble hat Verfahren für die Verwaltung von Kennwörtern für dieses demografische Personal eingeführt und wird diese entsprechend pflegen, um sicherzustellen, dass die Kennwörter für jede Person eindeutig und für Unbefugte unzugänglich sind, darunter mindestens:

- Kryptografischer Schutz von Kennwörtern, die in Computersystemen gespeichert sind oder über ein öffentliches Netz übertragen werden
- Ändern von Standardkennwörtern von Anbietern
- Aufklärung über gute Kennwortpraktiken wie die Verwendung von Passphrasen

- Multi-Faktor-Authentifizierung (MFA) als Voraussetzung für den Zugriff der Mitarbeiter auf die Produktionsinfrastruktur

Zur Einhaltung des ISO 27001-Zertifikats und zur Gewährleistung eines ordnungsgemäßen und effektiven Einsatzes von Kryptographie zum Schutz der Vertraulichkeit und Integrität von Daten, die sich im Besitz von Trimble befinden oder von Trimble verwaltet werden, müssen Daten, die als vertraulich oder eingeschränkt eingestuft sind, durch den Einsatz gültiger Verschlüsselungsprozesse für ruhende und bewegte Daten verschlüsselt werden, wie es die Vorschriften und/oder die Risikobewertung erfordern. Dies gilt unter anderem für sensible Informationen, die auf Mobilgeräten, Wechsellaufwerken und Laptops gespeichert sind. Trimble verwendet nur unveränderte, kommerzielle Kryptografieanwendungen zur Verschlüsselung von Daten im Ruhezustand und/oder während der Übertragung.

Die Mitarbeiter von Trimble unterliegen Geheimhaltungsverpflichtungen und verschiedenen Richtlinien, z. B. der Richtlinie für akzeptable Nutzung, der Richtlinie zur Datenklassifizierung, der Richtlinie zur sicheren Datenvernichtung und der MFA-Richtlinie. Trimble verlangt von seinen Mitarbeitern, dass sie zu Beginn ihres Arbeitsverhältnisses und im weiteren Verlauf jährlich eine Schulung zum Thema Informationssicherheit absolvieren. Trimble verlangt von seinen Mitarbeitern außerdem, dass sie jährlich eine Datenschutzschulung absolvieren (auch zur Einhaltung der DSGVO).

Für die entsprechenden Produkte hat Trimble die Prinzipien der eingebauten Sicherheit und Privatsphäre (Security and Privacy by Design) umgesetzt, darunter Bedrohungsmodellierung und Penetrationstests für Produktanwendungen.

12. Maßnahmen zur Zertifizierung/Absicherung von Prozessen und Produkten

Trimble sorgt dafür, dass die Zertifizierungen SOC 2, Typ II, ISO 27001 oder NIST 800-171 erhalten bleiben, und unterzieht sich regelmäßigen externen Überwachungs- und Rezertifizierungsaudits, um sicherzustellen, dass sein Informationssicherheitsmanagementsystem (ISMS) die Anforderungen dieses Standards für die entsprechenden Produkte erfüllt.

Trimble unterhält Richtlinien zur Informationssicherheit, die den Anforderungen der Norm ISO 27001 entsprechen, ein internes Auditprogramm, mit dem das ISMS und die Informationssicherheitskontrollen von Trimble bewertet werden, sowie ein Managementteam, das für die Überwachung des Informationssicherheitsmanagementsystems (ISMS) von Trimble verantwortlich ist.

13. Maßnahmen zur Gewährleistung der Datensparsamkeit

Trimble kann Besuchern die anonyme Nutzung bestimmter Funktionen einiger Produkte gestatten und beschränkt die von den Kunden benötigten Daten auf das, was für die Erbringung des angeforderten Dienstes gemäß den lokalen Gesetzen und Vorschriften erforderlich ist.

14. Maßnahmen zur Sicherung der Datenqualität

Trimble stellt die Qualität seiner Daten durch verschiedene Verifizierungsmechanismen sicher, die nur für die jeweiligen Trimble-Produkte gelten. Trimble kann Produktbenutzern außerdem gestatten, die Informationen in ihren Konten selbst oder durch Anfragen an den Kundendienst zu aktualisieren.

15. Maßnahmen zur Gewährleistung einer begrenzten Datenspeicherung

Trimble kann die Datenaufbewahrungsrichtlinie des Kunden umsetzen, in der die Aufbewahrungsfristen für verschiedene Arten von Daten festgelegt sind.

16. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Datenlöschung

Relevante Trimble-Produkte verfügen über ein Verfahren zur Löschung von Kundendaten innerhalb von 30 Tagen nach Erhalt einer verifizierten schriftlichen Anfrage des Kunden und können das Herunterladen von Kundendaten ermöglichen, um sie gemäß den Anforderungen der DSGVO alternativen Dienstanbietern zur Verfügung zu stellen.

17. Kontrolle und Verwaltung von Dritten (Unterauftragsverarbeitern)

Trimble setzt nur Unterauftragsverarbeiter ein, die personenbezogene Daten im Auftrag von Trimble im Rahmen der anwendbaren Abonnementdienste unter Einhaltung der Datenschutzgesetze und -vorschriften verarbeiten. Trimble prüft außerdem vor der Auswahl eines Unterauftragsverarbeiters und der Übermittlung von Daten die technischen und organisatorischen Maßnahmen des Unterauftragsverarbeiters, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko der Datenverarbeitung seiner Kunden angemessen ist. Trimble ergreift zudem angemessene Maßnahmen, um die Sicherheit der Übermittlung von Kundendaten an dritte

Unterauftragsverarbeiter zu gewährleisten. Diese Maßnahmen umfassen mindestens die Identifizierung der Risiken für die Rechte des Kunden und des Datensubjekts auf der Grundlage der Art, des Umfangs und des Kontexts der Verarbeitung, die Überprüfung der Sicherheits- und Datenschutzkontrollen, die vom Unterauftragsverarbeiter zum Schutz der Kundendaten durchgeführt werden (einschließlich SOC 2 Typ II-Auditberichte und/oder ISO 27001-Zertifikate, soweit anwendbar), Auferlegung von Datenschutzvertragsbedingungen, die personenbezogene Daten nach demselben oder einem ähnlichen Standard schützen, den Trimble seinen Kunden bereitzustellen verpflichtet ist (einschließlich gültiger Mechanismen für grenzüberschreitende Übermittlungen, Verwaltung des Unterauftragsverarbeiters und Compliance-Programme), Verpflichtung des Unterauftragsverarbeiters, Kundendaten nur im Auftrag von Trimble und seinen Kunden zu verarbeiten, sowie Beschränkung seiner Verarbeitung von Kundendaten auf den Umfang der Vorgaben von Trimble.

ANHANG 3 - Grenzüberschreitender Übermittlungsmechanismus

1. Europäischer Wirtschaftsraum (EWR):

1.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ umfasst die Datenschutz-Grundverordnung (EU 2016/679) („***DSGVO***“).

1.2 Wenn Trimble einen Unterauftragsverarbeiter gemäß Abschnitt 5.1 (Beauftragung von Unterauftragsverarbeitern) dieser DVV beauftragt, macht Trimble folgende Vorgaben:

(a) Trimble verlangt von allen beauftragten Unterauftragsverarbeitern, dass sie die Kundendaten gemäß den Datenschutzgesetzen und -vorschriften schützen, und erlegt ihnen dieselben Datenschutzverpflichtungen auf, auf die in Artikel 28(3) der DSGVO verwiesen wird, insbesondere ausreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, damit die Verarbeitung den Anforderungen der DSGVO entspricht.

(b) Trimble verlangt von allen beauftragten Unterauftragsverarbeitern, dass sie (i) sich schriftlich verpflichten, personenbezogene Daten nur in einem Land zu verarbeiten, das von der Europäischen Union als Land mit „angemessenem“ Schutzniveau eingestuft wurde, oder (ii) personenbezogene Daten nur auf der Grundlage der EU-Standardvertragsklauseln oder gemäß den von den zuständigen Datenschutzbehörden der Europäischen Union genehmigten verbindlichen Unternehmensregeln (Binding Corporate Rules, BCR) zu verarbeiten.

1.3 Ungeachtet gegenteiliger Bestimmungen in dieser DVV oder im Vertrag (darunter die Entschädigungsverpflichtungen der Parteien) ist keine der Parteien für Geldbußen gemäß Artikel 83 der DSGVO verantwortlich, die von einer Aufsichtsbehörde oder staatlichen Stelle gegen die andere Partei im Zusammenhang mit einem Verstoß der anderen Partei gegen die DSGVO verhängt oder erhoben werden.

1.4 Der Kunde erkennt an, dass Trimble als Datenverantwortlicher gemäß den Datenschutzgesetzen und -vorschriften verpflichtet sein kann, eine Aufsichtsbehörde über Sicherheitsvorfälle mit Kundendaten zu informieren. Wenn eine Aufsichtsbehörde von Trimble verlangt, Datensubjekte zu benachrichtigen, zu denen Trimble keine direkte Beziehung hat (z. B. die Endbenutzer des Kunden), informiert Trimble den Kunden über diese Anforderung. Der Kunde unterstützt Trimble in angemessener Weise bei der Benachrichtigung der Datensubjekte.

2. United Kingdom (UK):

2.1 Verweise in dieser DVV auf die britische Datenschutz-Grundverordnung „GDPR“ gelten als Verweise auf die entsprechenden Gesetze und Vorschriften des United Kingdom, darunter auf die britische GDPR und den Data Protection Act 2018.

2.2 Wenn Trimble einen Unterauftragsverarbeiter gemäß Abschnitt 5.1 (Beauftragung von Unterauftragsverarbeitern) dieser DVV beauftragt, macht Trimble folgende Vorgaben:

(a) Trimble verlangt von allen beauftragten Unterauftragsverarbeitern, dass sie die Kundendaten gemäß den Datenschutzgesetzen und -vorschriften schützen, indem diesen dieselben Datenschutzverpflichtungen auferlegt werden, auf die in Artikel 28(3) der britischen Datenschutz-Grundverordnung verwiesen wird, insbesondere ausreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, damit die Verarbeitung den Anforderungen der britischen Datenschutz-Grundverordnung entspricht.

(b) Trimble verlangt von allen beauftragten Unterauftragsverarbeitern, dass sie (i) sich schriftlich verpflichten, personenbezogene Daten nur in einem Land zu verarbeiten, dem das United Kingdom ein „angemessenes“ Schutzniveau bescheinigt hat, oder (ii) personenbezogene Daten nur zu Bedingungen zu verarbeiten, die dem UK

International Data Transfer Agreement oder den EU-Standardvertragsklauseln und dem UK International Data Transfer Addendum gleichwertig sind, oder gemäß den verbindlichen Unternehmensregeln verbindlichen Unternehmensregeln (Binding Corporate Rules, BCR) zu verarbeiten, die von den zuständigen britischen Datenschutzbehörden genehmigt wurden.

2.3 Ungeachtet gegenteiliger Bestimmungen in dieser DVV oder im Vertrag (darunter die Entschädigungsverpflichtungen der Parteien) ist keine der Parteien für Geldbußen gemäß Artikel 83 der britischen Datenschutz-Grundverordnung verantwortlich, die von einer Aufsichtsbehörde oder staatlichen Stelle gegen die andere Partei im Zusammenhang mit einem Verstoß der anderen Partei gegen die britischen Datenschutz-Grundverordnung verhängt oder erhoben werden.

2.4 Der Kunde erkennt an, dass Trimble als Datenverantwortlicher gemäß den Datenschutzgesetzen und -vorschriften verpflichtet sein kann, eine Aufsichtsbehörde über Sicherheitsvorfälle mit Kundendaten zu informieren. Wenn eine Aufsichtsbehörde von Trimble verlangt, Datensubjekte zu benachrichtigen, zu denen Trimble keine direkte Beziehung hat (z. B. die Endbenutzer des Kunden), informiert Trimble den Kunden über diese Anforderung. Der Kunde unterstützt Trimble in angemessener Weise bei der Benachrichtigung der Datensubjekte.

3. Schweiz:

3.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ umfasst das Schweizerische Bundesgesetz über den Datenschutz in seiner revidierten Fassung („***DSG***“).

3.2 Wenn Trimble einen Unterauftragsverarbeiter gemäß Abschnitt 5.1 (Beauftragung von Unterauftragsverarbeitern) dieser DVV beauftragt, macht Trimble folgende Vorgaben:

(a) Trimble verlangt von allen beauftragten Unterauftragsverarbeitern, dass sie die Kundendaten gemäß den Datenschutzgesetzen und -vorschriften schützen und insbesondere ausreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bieten, damit die Verarbeitung den Anforderungen des DSG entspricht.

(b) Trimble verlangt von allen beauftragten Unterauftragsverarbeitern, dass sie (i) sich schriftlich verpflichten, personenbezogene Daten nur in einem Land zu verarbeiten, das von der Schweiz als Land mit „angemessenem“ Schutzniveau eingestuft wurde, oder (ii) personenbezogene Daten nur zu Bedingungen zu verarbeiten, die den EU-Standardvertragsklauseln einschließlich der in Abschnitt 3.3 genannten Änderungen gleichwertig sind, oder gemäß den von den zuständigen Datenschutzbehörden der Europäischen Union oder der Schweiz genehmigten verbindlichen Unternehmensregeln (Binding Corporate Rules, BCR) zu verarbeiten.

3.3 Soweit die Übermittlung personenbezogener Daten aus der Schweiz den EU-Standardvertragsklauseln gemäß Abschnitt 2.3 des Anhangs 3 (EU-Standardvertragsklauseln) unterliegt, vereinbaren die Parteien, dass alle vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) für notwendig erachteten Änderungen an den EU-Standardvertragsklauseln erfolgen. Zum Zeitpunkt des Abschlusses der DVV sind dies:

(a) Verweise auf „EU-Mitgliedstaat“ und „Mitgliedstaat“ sind so auszulegen, dass sie die Schweiz einschließen.

(b) Soweit die Übermittlung oder Weiterübermittlung dem DSG unterliegt:

(i) Verweise auf die „Verordnung (EU) 2016/679“ sind als Verweise auf das DSG zu verstehen.

(ii) Die „zuständige Aufsichtsbehörde“ in Anhang I, Teil C ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

(iii) In Bezug auf Klausel 17 (Option 1) unterliegen die EU-Standardvertragsklauseln dem belgischen Recht.

(iv) In Bezug auf Klausel 18(b) der EU-Standardvertragsklauseln gilt, dass für Streitigkeiten die Gerichte der Schweiz zuständig sind.

(v) Klausel 18(c) der EU-Standardvertragsklauseln findet Anwendung, wobei ein Datensubjekt den Datenexporteur und/oder Datenimporteur auch vor den Gerichten der Schweiz verklagen kann, in der das Datensubjekt seinen gewöhnlichen Aufenthaltsort hat.

4. Vereinigte Staaten von Amerika:

4.1 ***„Datenschutzgesetze der US-Bundesstaaten***“ bezieht sich auf alle bundesstaatlichen Gesetze in Bezug auf den Schutz und die Verarbeitung personenbezogener Daten, die in den USA in Kraft sind, wozu unter anderem die folgenden Verbraucherschutzgesetze gehören können: California Consumer Privacy Act, der durch den California Privacy Rights Act („***CCPA***“) geändert wurde, Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act und Utah Consumer Privacy Act.

4.2 Die Definition von „Datenschutzgesetzen und -vorschriften“ umfasst die Datenschutzgesetze der US-Bundesstaaten.

4.3 Die folgenden Bestimmungen gelten, wenn Trimble personenbezogene Daten verarbeitet, die dem CCPA unterliegen:

(a) Der Begriff „***personenbezogene Daten***“, wie er in diesem Abschnitt 4.3 verwendet wird, hat die im CCPA festgelegte Bedeutung.

(b) Trimble ist bei der Verarbeitung von Kundendaten ein Dienstanbieter. Trimble verarbeitet die in den Kundendaten enthaltenen personenbezogenen Daten nur für die in der Vereinbarung festgelegten Geschäftszwecke, einschließlich des Zwecks der Verarbeitung und der in dieser DVV festgelegten Verarbeitungstätigkeiten („Zweck“). Als Dienstanbieter werden von Trimble keine Kundendaten verkauft, weitergegeben aufbewahrt, verwendet oder offengelegt (i) für einen anderen Zweck als den eigentlichen Zweck, einschließlich der Aufbewahrung, Verwendung oder Offenlegung von Kundendaten für einen anderen kommerziellen Zweck als den eigentlichen Zweck, oder wie anderweitig durch den CCPA erlaubt, oder (ii) außerhalb der direkten Geschäftsbeziehung zwischen dem Kunden und Trimble.

(c) Trimble erfüllt (i) die Verpflichtungen, die für Trimble als Dienstanbieter gemäß dem CCPA gelten, und (ii) wendet für personenbezogene Daten dasselbe Datenschutzniveau an, das durch den CCPA vorgeschrieben ist. Der Kunde ist dafür verantwortlich, dass er bei seiner Nutzung der Dienste und seiner eigenen Verarbeitung personenbezogener Daten die Anforderungen des CCPA erfüllt und weiterhin erfüllen wird.

(d) Der Kunde hat das Recht, angemessene und geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass Trimble personenbezogene Daten in einer Weise verwendet, die mit den Verpflichtungen des Kunden gemäß dem CCPA vereinbar ist.

(e) Trimble informiert den Kunden, wenn Trimble zu dem Schluss kommt, den Verpflichtungen als Dienstanbieter im Rahmen des CCPA nicht mehr nachkommen zu können.

(f) Nach einer entsprechenden Benachrichtigung hat der Kunde das Recht, angemessene und geeignete Schritte in Übereinstimmung mit der Vereinbarung zu unternehmen, um die unbefugte Nutzung personenbezogener Daten zu stoppen und zu beheben.

(g) Trimble wird dem Kunden in angemessenem Umfang zusätzliche und zeitnahe Unterstützung bei der Erfüllung seiner Verpflichtungen in Bezug auf Verbraucheranfragen gemäß der Vereinbarung gewähren.

(h) Bei allen Unterauftragsverarbeitern, die Trimble zur Verarbeitung personenbezogener Daten einsetzt und die dem CCPA unterliegen, stellt Trimble sicher, dass die Vereinbarung zwischen Trimble und dem Unterauftragsverarbeiter die CCPA-Bestimmungen erfüllt, darunter die vertraglichen Anforderungen für Dienstanbieter und Auftragnehmer.

(i) Trimble kombiniert Kundendaten, die Trimble vom Kunden oder im Namen des Kunden erhält, nicht mit personenbezogenen Daten, die Trimble von einer oder mehreren anderen Personen oder im Namen einer anderen Person erhält oder die Trimble im Rahmen seiner eigenen Interaktion mit dem Verbraucher sammelt, es sei denn, eine solche Kombination ist erforderlich, um einen Geschäftszweck zu erfüllen, der durch den CCPA, einschließlich der zugehörigen Vorschriften oder durch die von der kalifornischen Datenschutzbehörde erlassenen Vorschriften erlaubt ist.

(j) Trimble bestätigt, dass Trimble seine Verpflichtungen aus dem CCPA kennt und einhalten wird.

4.4 Trimble erkennt an und bestätigt, dass Trimble Kundendaten nicht als Gegenleistung für die dem Kunden erbrachten Dienste erhält.

5. Australien:

5.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ umfasst die australischen Datenschutzgrundsätze (Australian Privacy Principles, APPs) und den Australian Privacy Act (1988).

5.2 Die Definition des Begriffs „personenbezogene Daten“ umfasst „persönliche Informationen“ im Sinne der Datenschutzgesetze und -vorschriften.

5.3 Die Definition von „sensiblen Daten“ umfasst „sensible Informationen“ gemäß der Definition in den Datenschutzgesetzen und -vorschriften.

6. Brasilien:

6.1 Die Definition des Begriffs „Datenschutzgesetze und -vorschriften“ umfasst das brasilianische Lei Geral de Proteção de Dados (Allgemeines Datenschutzgesetz).

6.2 Die Definition des Begriffs „Sicherheitsvorfall“ umfasst einen Sicherheitsvorfall, der zu einem relevanten Risiko oder Schaden für die Datensubjekte führen kann.

6.3 Die Definition des Begriffs „Auftragsverarbeiter“ schließt den Begriff „Betreiber“ im Sinne der Datenschutzgesetze und -vorschriften ein.

7. Kanada:

7.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ umfasst das kanadische Bundesgesetz zum Schutz personenbezogener Daten und elektronischer Dokumente (Federal Personal Information Protection and Electronic Documents Act).

7.2 Die Unterauftragsverarbeiter von Trimble sind gemäß Abschnitt 5 (Unterauftragsverarbeiter) dieser DVV Drittparteien im Sinne der Datenschutzgesetze und -vorschriften, mit denen Trimble einen schriftlichen Vertrag abgeschlossen hat, der im Wesentlichen ähnliche Bedingungen wie diese DVV enthält. Trimble hat eine angemessene Due-Diligence-Prüfung seiner Unterauftragsverarbeiter durchgeführt.

7.3 Trimble ergreift technische und organisatorische Maßnahmen gemäß Abschnitt 11 von Anhang 2 (Sicherheit) dieser DVV.

8. Israel:

8.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ schließt das israelische Datenschutzgesetz ein.

8.2 Die Definition des Begriffs „Datenverantwortlicher“ schließt den Begriff „Datenbankinhaber“ im Sinne der Datenschutzgesetze und -vorschriften ein.

8.3 Die Definition des Begriffs „Auftragsverarbeiter“ schließt den Begriff „Inhaber“ im Sinne der Datenschutzgesetze und -vorschriften ein.

8.4 Trimble verlangt, dass alle zur Verarbeitung von Kundendaten befugten Mitarbeiter den Grundsatz des Datengeheimnisses einhalten und ordnungsgemäß über die Datenschutzgesetze und -vorschriften unterrichtet wurden. Diese Mitarbeiter unterzeichnen Vertraulichkeitsvereinbarungen mit Trimble in Übereinstimmung mit Abschnitt 6 („Vertraulichkeit“) dieser DVV.

8.5 Trimble muss ausreichende Maßnahmen ergreifen, um den Schutz der Privatsphäre der Datensubjekte zu gewährleisten, indem es die in Abschnitt 11 von Anhang 2 (Sicherheit) dieser DVV genannten Sicherheitsmaßnahmen umsetzt und beibehält und die Bedingungen der Vereinbarung einhält.

8.6 Trimble muss sicherstellen, dass die personenbezogenen Daten nicht an einen Unterauftragsverarbeiter übermittelt werden, sofern der Unterauftragsverarbeiter mit Trimble keine Vereinbarung gemäß Abschnitt 5.1 (Beauftragung von Unterauftragsverarbeitern) dieser DVV abgeschlossen hat.

9. Japan:

9.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ schließt das japanische Datenschutzgesetz („***APPI***“) ein.

9.2 Die Definition des Begriffs „personenbezogene Daten“ umfasst Daten über eine bestimmte Person, die gemäß Abschnitt 2(1) des APPI anwendbar sind und die der Kunde Trimble bei der Erbringung der Dienstleistungen für den Kunden anvertraut.

9.3 Trimble erklärt sich damit einverstanden, dass es ein Datenschutzprogramm hat und aufrechterhält, das den Standards entspricht, die in den Vorschriften der japanischen Personal Information Protection Commission für den Umgang mit personenbezogenen Daten gemäß den Bestimmungen von Kapitel 4 des APPI vorgeschrieben sind. Diesbezüglich gilt:

(a) Trimble verarbeitet (i) personenbezogene Daten in dem Maße, wie es für die Erbringung der Dienste für den Kunden in Übereinstimmung mit der Vereinbarung und gemäß Anhang 1 (Beschreibung der Verarbeitung) dieser DVV („*Zweck der Verarbeitung*“) festgelegt ist, und (ii) verarbeitet personenbezogene Daten ohne Zustimmung des Kunden nicht für andere Zwecke als den Zweck der Verarbeitung.

(b) Trimble ergreift und pflegt Maßnahmen, die geeignet und notwendig sind, um die unbefugte Offenlegung und den Verlust personenbezogener Daten zu verhindern und die sichere Verwaltung personenbezogener Daten in Übereinstimmung mit dem APPI zu gewährleisten, wie in Anhang 2 (Technische und organisatorische Sicherheitsmaßnahmen) dieser DVV dargelegt.

(c) Trimble informiert den Kunden (i) bei Nichteinhaltung von Abschnitt 9.3(a) dieses Anhangs 3 oder (ii) bei Entdeckung eines Sicherheitsvorfalls durch Trimble, der sich auf Kundendaten auswirkt, in beiden Fällen gemäß Abschnitt 6.4 dieser DVV. Trimble unterstützt den Kunden in angemessener Weise, wenn der Kunde verpflichtet ist, eine Aufsichtsbehörde oder von einem Sicherheitsvorfall betroffene Datensubjekte zu informieren.

(d) Trimble stellt sicher, dass alle seine Mitarbeiter, die Zugang zu personenbezogenen Daten haben, (i) Mitarbeitervereinbarungen abgeschlossen haben, die sie zur vertraulichen Behandlung dieser personenbezogenen Daten verpflichten, und (ii) dass Verstöße gegen die Vertraulichkeit durch Disziplinarmaßnahmen und gegebenenfalls durch Kündigung geahndet werden; (iii) eine angemessene Mitarbeiterbetreuung und -schulung im Hinblick auf die sichere Verwaltung personenbezogener Daten erhalten, und (iv) die Anzahl der befugten Personen, einschließlich der Mitarbeiter von Trimble, die Zugang zu personenbezogenen Daten haben, begrenzen und diesen Zugang so kontrollieren, dass er nur für den für den Zweck der Verarbeitung erforderlichen Zeitraum gewährt wird.

(e) Trimble gibt keine personenbezogenen Daten an Dritte weiter, sofern der Kunde Trimble im Rahmen der Vereinbarung nicht dazu ermächtigt. Bei der Beauftragung von Unterauftragsverarbeitern hält Trimble die Verpflichtungen in Abschnitt 9 (Unterauftragsverarbeiter) dieser DVV ein, um zu gewährleisten, dass es entsprechende Verfahren zur Wahrung der Vertraulichkeit und Sicherheit personenbezogener Daten vorhanden gibt.

(f) Trimble führt Aufzeichnungen über den Umgang mit personenbezogenen Daten, die Trimble vom Kunden anvertraut wurden und die von Trimble für den Kunden verarbeitet werden.

(g) Der Kunde ist berechtigt, die Einhaltung der Verpflichtungen von Trimble gemäß den Datenschutzgesetzen und -vorschriften sowie gemäß Abschnitt 6 dieser DVV zu beurteilen.

(h) Trimble ist dem Kunden auf schriftliche Anfrage in angemessener Weise behilflich, wenn der Kunde der japanischen Personal Information Protection Commission oder anderen Aufsichtsbehörden Bericht erstattet.

(i) Die primären Datenverarbeitungseinrichtungen von Trimble befinden sich in den USA und, je nach Nutzung der Dienste durch den Kunden, an den Standorten, die bei https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center unter „Additional Resources“ („Sub-processor Lists“) aufgeführt sind. Trimble informiert den Kunden über jede Änderung und gibt ihm die Möglichkeit, gemäß Abschnitt 9 dieser DVV Widerspruch einzulegen. Wenn Trimble personenbezogene Daten in einem anderen Land als Japan verarbeitet, stellt Trimble sicher, dass sein Datenschutzprogramm gemäß dieser DVV einzuhalten.

9.4 Es gelten die folgenden Bedingungen für die Zustimmung des Datensubjekts:

(a) Der Kunde vertraut Trimble personenbezogene Daten zum Zweck der Verarbeitung an. Der Kunde erkennt an, dass Trimble keine „Drittpartei“ im Sinne der APPI-Bestimmungen ist, die die Weitergabe von personenbezogenen

Daten an Dritte einschränken. Daher gilt die Anforderung nicht, die Zustimmung des Datensubjekts im Voraus einzuholen.

(b) Wenn die Zustimmung des Datensubjekts gemäß Artikel 4 des japanischen Telekommunikationsgesetzes erforderlich ist, erfüllt der Kunde alle Zustimmungsanforderungen, die für seine Nutzung der Dienste gelten.

10. Mexiko:

10.1 Die Definition des Begriffs „Datenschutzgesetze und -vorschriften“ umfasst das mexikanische Datenschutzgesetz.

10.2 Wenn Trimble als Auftragsverarbeiter handelt, gilt Folgendes:

(a) Trimble behandelt personenbezogene Daten gemäß den Anweisungen des Kunden in Abschnitt 5 dieser DVV.

(b) Trimble verarbeitet personenbezogene Daten nur in dem Umfang, der für die Erbringung der Dienste erforderlich ist.

(c) Trimble setzt Sicherheitsmaßnahmen in Übereinstimmung mit den Datenschutzgesetzen und -verordnungen sowie Anhang 2 (Technische und organisatorische Sicherheitsmaßnahmen) dieser DVV um.

(d) Trimble behandelt die verarbeiteten personenbezogenen Daten gemäß dieser Vereinbarung vertraulich.

(e) Trimble löscht alle personenbezogenen Daten bei Beendigung der Vereinbarung gemäß Abschnitt 10 (Rückgabe und Löschung von Kundendaten) dieser DVV.

(f) Trimble übermittelt personenbezogene Daten an Unterauftragsverarbeiter nur gemäß Abschnitt 9 (Unterauftragsverarbeiter) dieser DVV.

11. Singapur:

11.1 Die Definition von „Datenschutzgesetzen und -vorschriften“ schließt den Personal Data Protection Act 2012 („***PDPA***“) ein.

11.2 Trimble verarbeitet personenbezogene Daten gemäß dem PDPA, indem es angemessene technische und organisatorische Maßnahmen gemäß Anhang 2 (Technische und organisatorische Sicherheitsmaßnahmen) dieser DVV ergreift und die Bedingungen der Vereinbarung einhält.

12. Türkei

12.1 Die Definition des Begriffs „Datenschutzgesetze und -vorschriften“ umfasst (i) das türkische Datenschutzgesetz („PDPL“), Gesetz Nr. 6698 vom 24. März 2016, geändert durch das Gesetz zur Änderung der Strafprozessordnung und anderer Gesetze, Gesetz Nr. 7499 vom 2. März 2024, und (ii) die Verordnung über Grundsätze zu Verfahren und Regeln für die Übermittlung personenbezogener Daten ins Ausland von der Datenschutzbehörde, veröffentlicht im türkischen Amtsblatt vom 10. Juli, Nr. 32598.

12.2 Der Kunde erkennt an, dass Trimble als Datenverantwortlicher gemäß den Datenschutzgesetzen und -vorschriften verpflichtet sein kann, eine Aufsichtsbehörde über Sicherheitsvorfälle mit Kundendaten zu informieren. Wenn eine Aufsichtsbehörde von Trimble verlangt, Datensubjekte zu benachrichtigen, zu denen Trimble keine direkte Beziehung hat (z. B. die Endbenutzer des Kunden), informiert Trimble den Kunden über diese Anforderung. Der Kunde unterstützt Trimble in angemessener Weise bei der Benachrichtigung der Datensubjekte.

ANHANG 4 - GRENZÜBERSCHREITENDER ÜBERMITTLUNGSMECHANISMUS
(Gilt für Daten, die aus der EU, dem EWR, dem United Kingdom und der Schweiz übermittelt werden)

1. Definitionen

- ***„EU-Standardvertragsklauseln“*** beziehen sich auf die Standardvertragsklauseln, die von der Europäischen Kommission mit dem Durchführungsbeschluss 2021/914 genehmigt wurden.
- ***„UK International Data Transfer Agreement“*** bezieht sich auf das International Data Transfer Addendum zu den Standardvertragsklauseln der EU-Kommission, herausgegeben vom UK Information Commissioner, Version B1.0, und in Kraft seit dem 21. März 2022.
- „Data Privacy Framework“ bezeichnet das vom US-Handelsministerium betriebene Selbstzertifizierungsprogramm für das EU-U.S. DPF und/oder das Swiss-U.S. DPF.
- ***„Datenschutzgrundsätze“*** bezeichnet die Vorgaben des Data Privacy Framework (ergänzt durch die ergänzenden Grundsätze bzw. Supplemental Principles).
- ***„Türkische Standardvertragsklauseln“*** bezieht sich auf die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer 1–4, die durch den Beschluss 2024/959 vom 4. Juni 2024 von der türkischen Datenschutzbehörde angenommen wurden.

2. Grenzüberschreitende Datenübermittlungsmechanismen

2.1 Rangfolge: Falls die Dienste von mehr als einem Übermittlungsmechanismus abgedeckt werden, unterliegt die Übermittlung personenbezogener Daten einem einzigen Übermittlungsmechanismus, je nach Anwendbarkeit und in Übereinstimmung mit der folgenden Rangfolge: (a) Data Privacy Framework gemäß Abschnitt 2.2 (Data Privacy Framework) dieses Anhangs, (b) EU-Standardvertragsklauseln gemäß Abschnitt 2.3 (EU-Standardvertragsklauseln) dieses Anhangs, (c) UK International Data Transfer Addendum gemäß Abschnitt 2.4 (UK International Data Transfer Addendum) dieses Anhangs, und falls weder (a), (b), (c), (d) noch (e) anwendbar sind, dann (f) andere anwendbare Datenübermittlungsmechanismen, die nach den Datenschutzgesetzen und -vorschriften zulässig sind.

2.2 Data Privacy Framework: Soweit Trimble Inc. über die Dienste personenbezogene Daten verarbeitet, die aus dem EWR oder der Schweiz stammen, ist Trimble Inc. gemäß dem Data Privacy Framework selbstzertifiziert und hält sich bei der Verarbeitung dieser personenbezogenen Daten an die Datenschutzgrundsätze. Soweit der Kunde (a) in den USA ansässig ist und sich ebenfalls nach dem Data Privacy Framework selbstzertifiziert hat oder (b) im EWR oder in der Schweiz ansässig ist, verpflichtet sich Trimble außerdem, (i) mindestens das gleiche Schutzniveau für personenbezogene Daten zu gewährleisten, wie es die Datenschutzgrundsätze verlangen, (ii) den Kunden unverzüglich schriftlich zu benachrichtigen, wenn seine Selbstzertifizierung gemäß den Datenschutzgrundsätzen zurückgenommen, beendet, widerrufen oder anderweitig für ungültig erklärt wird (in diesem Fall gilt ein alternativer Übermittlungsmechanismus gemäß der Rangfolge in Abschnitt 2.1 (Rangfolge) dieses Anhangs 4, und (iii) nach schriftlicher Mitteilung in Zusammenarbeit mit dem Kunden angemessene und geeignete Maßnahmen zu ergreifen, um die unbefugte Verarbeitung personenbezogener Daten zu stoppen und zu beheben.

2.3 EU-Standardvertragsklauseln: Die EU-Standardvertragsklauseln gelten für personenbezogene Daten, die über die Dienste aus dem EWR, der Schweiz oder dem United Kingdom entweder direkt oder auf dem Wege der Weiterübermittlung in ein Land oder einen Empfänger außerhalb des EWR, der Schweiz oder des United Kingdom übermittelt werden, das bzw. der von der jeweils zuständigen Behörde nicht als Land anerkannt ist, das ein angemessenes Schutzniveau für personenbezogene Daten bietet. Für Datenübermittlungen, die den EU-Standardvertragsklauseln unterliegen, gelten die EU-Standardvertragsklauseln als anwendbar und werden durch diesen Verweis in diese DVV aufgenommen und wie folgt ergänzt:

(a) Modul 1 (Datenübermittlung zwischen zwei Datenverantwortlichen) der EU-Standardvertragsklauseln findet Anwendung, wenn (i) Trimble die Daten des Kundenkontos verarbeitet und (ii) der Kunde ein Datenverantwortlicher der Kundennutzungsdaten ist und Trimble die Kundennutzungsdaten verarbeitet.

(b) Modul 2 (Datenübermittlung von einem Datenverantwortlichen an Auftragsverarbeiter) der EU-Standardvertragsklauseln findet Anwendung, wenn der Kunde ein Datenverantwortlicher der personenbezogenen Daten ist und Trimble personenbezogene Daten im Namen des Kunden verarbeitet.

(c) Modul drei (Datenübermittlung von einem Auftragsverarbeiter an einen anderen Auftragsverarbeiter) der EU-Standardvertragsklauseln findet Anwendung, wenn der Kunde ein Auftragsverarbeiter personenbezogener Daten ist und Trimble als Unterauftragsverarbeiter im Namen des Kunden Daten verarbeitet.

(d) Für jedes Modul gilt, sofern zutreffend:

(i) In Bezug auf Klausel 7 der EU-Standardvertragsklauseln ist die fakultative Andockklausel nicht anwendbar.

(ii) In Bezug auf Klausel 9 der EU-Standardvertragsklauseln gilt Option 2, und die Frist für die vorherige schriftliche Mitteilung von Änderungen des Unterauftragsverarbeiters ist in Abschnitt 5.2 (Liste der derzeitigen Unterauftragsverarbeiter und Meldung neuer Unterauftragsverarbeiter) dieser DVV festgelegt.

(iii) In Bezug auf Klausel 11 der EU-Standardvertragsklauseln ist die fakultative Sprache nicht anwendbar.

(iv) Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13;

(v) In Bezug auf Klausel 17 (Option 1) unterliegen die EU-Standardvertragsklauseln dem belgischen Recht.

(vi) In Bezug auf Klausel 18(b) der EU-Standardvertragsklauseln sind für Streitigkeiten die Gerichte in Amsterdam in den Niederlanden zuständig.

(vii) In Bezug auf Anhang I Teil A der EU-Standardvertragsklauseln gilt:

Datenexporteur: Kunde (wenn das Kästchen auf Seite 6 angekreuzt ist).

Kontaktangaben: Die E-Mail-Adresse(n), die der Kunde in seinem Konto über seine Benachrichtigungseinstellungen angegeben hat.

Rolle des Datenexporteurs: Die Rolle des Datenexporteurs ist auf Seite 6 beschrieben.

Unterschrift und Datum: Durch den Abschluss des Vertrags wird davon ausgegangen, dass der Datenexporteur diese hierin enthaltenen EU-Standardvertragsklauseln einschließlich ihrer Anhänge zum Zeitpunkt des Inkrafttretens des Vertrags unterzeichnet hat.

Datenimporteur: Trimble Inc.

Kontaktangaben: Trimble Privacy Team – privacy@Trimble.com

Rolle des Datenimporteurs: Die Rolle des Datenimporteurs ist auf Seite 6 beschrieben.

Unterschrift und Datum: Durch den Abschluss des Vertrags wird davon ausgegangen, dass der Datenimporteur diese hierin enthaltenen EU-Standardvertragsklauseln einschließlich ihrer Anhänge zum Zeitpunkt des Inkrafttretens des Vertrags unterzeichnet hat.

(viii) In Bezug auf Anhang I Teil B der EU-Standardvertragsklauseln gilt:

Die Kategorien der betroffenen Personen (Datensubjekte) sind in Abschnitt 1 von Anhang 1 (Beschreibung der Verarbeitung) dieser DVV aufgeführt.

Die übermittelten sensiblen Daten sind in Abschnitt 3 von Anhang 1 (Beschreibung der Verarbeitung) dieser DVV aufgeführt.

Die Häufigkeit der Übermittlung erfolgt kontinuierlich während der Vertragslaufzeit.

Die Art der Verarbeitung ist in Abschnitt 5 von Anhang 1 (Beschreibung der Verarbeitung) dieser DVV dargelegt.

Der Zweck der Verarbeitung ist in Abschnitt 6 von Anhang 1 (Beschreibung der Verarbeitung) dieser DVV dargelegt.

Die Aufbewahrungsdauer der personenbezogenen Daten ist in Abschnitt 7 von Anhang 1 (Beschreibung der Verarbeitung) dieser DVV festgelegt.

Bei Übermittlungen an Unterauftragsverarbeiter sind Gegenstand, Art und Dauer der Verarbeitung bei https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center unter „Additional Resources“ („Sub-processor Lists“) aufgeführt.

(ix) In Bezug auf Anhang I, Teil C der EU-Standardvertragsklauseln gilt: Sofern anwendbar, ist die niederländische Datenschutzkommission die zuständige Aufsichtsbehörde. Wenn eine in der EU ansässige Trimble-Organisation der Datenexporteur ist, ist die zuständige Aufsichtsbehörde die Aufsichtsbehörde des Mitgliedstaats, in dem die Trimble-Organisation ansässig ist. Handelt es sich bei dem Kunden um den Datenexporteur, so ist die zuständige Aufsichtsbehörde die Aufsichtsbehörde des Mitgliedstaates, in dem der Kunde ansässig ist.

(x) Anhang 2 (Technische und organisatorische Sicherheitsmaßnahmen) dieser DVV dient als Anhang II der EU-Standardvertragsklauseln.

2.4 UK-Erweiterung des Data Privacy Frameworks und International Data Transfer Addendum. Der Kunde und Trimble vereinbaren, dass die UK-Erweiterung des Data Privacy Frameworks gilt, und dass in Ermangelung dessen die EU-Standardvertragsklauseln und das UK International Data Transfer Addendum zu den Standardvertragsklauseln der EU-Kommission in seiner neuesten Fassung auf personenbezogene Daten Anwendung finden, die über die Dienste aus dem United Kingdom entweder direkt oder auf dem Wege der Weiterübermittlung an ein Land oder einen Empfänger außerhalb des United Kingdom übermittelt werden, das bzw. der von der zuständigen britischen Aufsichtsbehörde oder Regierungsstelle für das United Kingdom nicht als ein angemessenes Schutzniveau für personenbezogene Daten anerkannt ist. Bei Datenübermittlungen aus dem United Kingdom, die den EU-Standardvertragsklauseln und dem UK International Data Transfer Addendum unterliegen, gelten die EU-Standardvertragsklauseln als angenommen und in diese DVV aufgenommen, wie in Abschnitt 2.3 dieses Anhangs 4 beschrieben, und das UK International Data Transfer Addendum gilt als angenommen und wird durch diesen Verweis in diese DVV aufgenommen und wie folgt ergänzt:

(a) In Tabelle 1 des UK International Data Transfer Addendums sind die Angaben des Kunden und von Trimble sowie die wichtigsten Kontaktinformationen in Abschnitt 2.3 (e)(vii) dieses Anhangs 3 aufgeführt.

(b) In Tabelle 2 des UK International Data Transfer Addendums sind Informationen über die Version der EU-Standardvertragsklauseln und ausgewählte Klauseln, denen das UK International Data Transfer Addendum beigefügt ist, in Abschnitt 2.3 (EU-Standardvertragsklauseln) dieses Anhangs 4 aufgeführt.

(c) In Tabelle 3 des UK International Data Transfer Addendums gilt:

(i) Die Liste der Parteien ist in Abschnitt 2.3(e)(vii) dieses Anhangs 3 aufgeführt.

(ii) Die Beschreibung der Übermittlung ist in Abschnitt 1 von Anhang 1 (Beschreibung der Verarbeitung) enthalten.

(iii) Anhang II befindet sich in Anhang 2 (Technische und organisatorische Sicherheitsmaßnahmen) dieser DVV.

(iv) Die Liste der Unterauftragsverarbeiter ist bei https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center unter „Additional Resources“ („Sub-processor Lists“) einsehbar.

(d) In Tabelle 4 des UK International Data Transfer Addendums können sowohl der Datenimporteur als auch der Datenexporteur das UK International Data Transfer Agreement gemäß den Bestimmungen des UK International Data Transfer Addendums beenden.

2.5 Türkische Standardvertragsklauseln. Die türkischen Standardvertragsklauseln gelten für personenbezogene Daten, die über die genutzten Dienste aus der Türkei entweder direkt oder im Wege der Weiterübermittlung in ein Land oder einen Empfänger außerhalb der Türkei übermittelt werden, das bzw. der von der zuständigen Behörde nicht als Land anerkannt ist, das ein angemessenes Schutzniveau für personenbezogene Daten bietet. Für Datenübermittlungen, die den türkischen Standardvertragsklauseln unterliegen, gelten die türkischen Standardvertragsklauseln als anwendbar und werden durch diesen Verweis in diese DVV aufgenommen und wie folgt ergänzt:

Für jedes Modul gilt, sofern zutreffend:

(i) In Bezug auf Artikel 8 von Vertrag 2 und Vertrag 3 der türkischen Standardvertragsklauseln gilt Option 2, und die Frist für die vorherige schriftliche Mitteilung von Änderungen des Unterauftragsverarbeiters ist in Abschnitt 5.2 (Liste der derzeitigen Unterauftragsverarbeiter und Meldung neuer Unterauftragsverarbeiter) dieser DVV festgelegt.

(ii) Die Parteien vereinbaren, dass der Kunde die zuständige türkische Datenschutzbehörde innerhalb von fünf (5) Werktagen über die Umsetzung der türkischen Standardvertragsklauseln informiert.

(iii) Der Datenimporteur ist: Trimble mit Adressen, Vor- und Nachname, Stellenbezeichnung und Kontaktdaten von Trimble und unterzeichnender Person, wie in der DVV angegeben.

(iv) Unterschrift und Datum: Durch den Abschluss der Vereinbarung wird davon ausgegangen, dass Trimble und der Datenexporteur diese hierin enthaltenen türkischen Standardvertragsklauseln einschließlich ihrer Anhänge zum Datum des Inkrafttretens der Vereinbarung unterzeichnet haben.

(v) Die in Anhang I der türkischen Standardvertragsklauseln geforderten Angaben sind in Anhang 1 dieser DVV aufgeführt:

(vi) Anhang 2 (Technische und organisatorische Sicherheitsmaßnahmen) dieser DVV dient als Anhang II der türkischen Standardvertragsklauseln.

(vii) Die Liste der Unterauftragsverarbeiter ist bei https://www.trimble.com/en/our-commitment/responsible-business/data-privacy-and-security/data-privacy-center unter „Additional Resources“ („Sub-processor Lists“) einsehbar.

2.6 Konflikte: Bei Widersprüchen oder Unstimmigkeiten zwischen den EU-Standardvertragsklauseln, dem UK International Data Transfer Agreement oder den türkischen Standardvertragsklauseln und anderen Bestimmungen dieser DVV, einschließlich Anhang 4 (Grenzüberschreitender Übermittlungsmechanismus) haben je nach Sachlage die Bestimmungen der EU-Standardvertragsklauseln bzw. des UK International Data Transfer Addendums und der türkischen Standardvertragsklauseln Vorrang.