Agreement Number: [redacted]

Muster Vertrag über die Verarbeitung Personenbezogener Daten im Auftrag
für Adobe Cloud Services
[mit EU Standardvertragsklauseln]

Dieser Muster Vertrag zur Verarbeitung personenbezogener Daten im Auftrag („AV-Vertrag") kann zwischen **Adobe Systems Software Ireland Limited** mit Sitz in 4-6 Riverwalk, City West Business Campus, Saggart D24, Dublin, Irland ("Adobe") und **Bildungseinrichtungen** abgeschlossen werden, welche dem Adobe Enterprise Term License Agreement zwischen dem Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften, Boltzmannstraße 1, 85748 Garching b. München, Deutschland mit der Adobe Vertragsnummer [redacted] („Rahmen-ETLA") als Teilnehmer beitreten. Das Rahmen ETLA gilt dann als Lizenzvereinbarung iSd AV-Vertrages und ein Teilnehmer, der diesen AV-Vertrag mit Adobe abschließt als Kunde iSd AV-Vertrages.

Mit diesem AV-Vertrag soll gewährleistet werden, dass die Parteien die anwendbaren Datenschutzgesetze und -bestimmungen für die kundenseitige Verwendung der Adobe Cloud Services einhalten. Die beigefügte Anlage 1 und der Anhang 1 ergänzen die Bedingungen dieses AV-Vertrages für die entsprechenden Adobe Cloud Services.

1) Begriffsbestimmungen.

Die folgenden Begriffe haben folgende Bedeutungen:

a) „Adobe Cloud Services" sind die On-demand Services und Managed Services, die Adobe dem Kunden bereitstellt.

b) "Datenschutzverletzung" bedeutet einen bestätigten unbefugten Zugriff durch Dritte oder eine bestätigte versehentliche oder unrechtmäßige Zerstörung, Verlust oder Änderung personenbezogener Daten.

c) „EWR" ist der europäische Wirtschaftsraum bestehend aus seinen Mitgliedstaaten.

d) „Europäische Datenschutzgesetze" sind die EU Datenschutzgrundverordnung (EG) 2016/679 („DSGVO"), die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 (zuletzt geändert durch Richtlinie 2009/136/EG) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy Richtlinie) und alle nationalen Gesetze der EU Mitgliedsstaaten, die diese Richtlinien sowie deren Änderungen oder Nachfolgeregelungen in nationales Recht überführt haben. Soweit der Teilnehmer der katholischen oder evangelischen Kirche angehört, gelten als Europäische Datenschutzgesetze darüber hinaus entsprechend das Gesetz über den Kirchlichen Datenschutz (KDG) bzw. das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

e) „EU – U.S. Privacy Shield" (EU-US Datenschutzschild) ist das Rahmenabkommen zwischen der Europäischen Kommission und dem US Handelsministerium zur Vereinbarung adäquater Datenschutzschutzprinzipien für den Transfer personenbezogener Daten aus der EU in die Vereinigten Staaten von Amerika.

f) „Lizenzvereinbarung" ist die Vereinbarung, unter welcher Adobe oder Adobe als Vertreter der Adobe Systems Pty Ltd (Adobe Australien) dem Kunden Adobe Cloud Services entweder direkt oder indirekt bereitstellt.

g) „Personenbezogene Daten" hat die Bedeutung gemäß der Europäischen Datenschutzgesetze.

h) „Weisung" bezeichnet jede dokumentierte Weisung – schriftlich oder mittels Dateneingabe –, die Adobe vom Kunden unter Lizenzvereinbarungen und diesem AV-Vertrag erhält.

i) „Verarbeitung" oder „verarbeiten" hat die Bedeutung wie in den Europäischen Datenschutzgesetzen.

[redacted]

j) „Standardvertragsklauseln" sind die Vereinbarung gemäß dem Beschluss der EU Kommission vom 5. Februar 2010 zu den Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern ohne angemessenes Datenschutzniveau, welche als Anlage 1 diesem AV-Vertrag beigefügt ist.

k) „Support Services" sind die anwendbaren Kundensupportleistungen unter der Lizenzvereinbarung.

Alle anderen Begriffe in dieser Vereinbarung über Auftragsverarbeitung, die hier nicht aufgeführt sind, haben die in der Lizenzvereinbarung angegebene Bedeutung.

2. Allgemeine Bestimmungen.

Geltungsbereich. Die Bestimmungen dieses AV-Vertrags gelten für die Verarbeitung personenbezogener Daten durch Adobe unter der jeweiligen Lizenzvereinbarung. Im Falle von Abweichungen zwischen diesem AV-Vertrag und der Lizenzvereinbarung gehen die Bestimmungen dieses AV-Vertrags vor. Bei Unstimmigkeiten zwischen diesem AV-Vertrag, den Standardvertragsklauseln und dem EU - U.S. Privacy Shield hat der EU - U.S. Privacy Shield Vorrang, es sei denn, der Kunde und Adobe haben die Standardvertragsklauseln für die Zwecke dieses Vertrags abgeschlossen; in diesem Fall haben die Standardvertragsklauseln Vorrang.

3. Verarbeitung und Kategorien personenbezogener Daten.

a) Adobe verarbeitet alle Kundendaten, die personenbezogene Daten enthalten können, an den auf der Website des Adobe Privacy Center beschriebenen Standorten: www.adobe.com/go/processing.

b) Details zur Verarbeitung personenbezogener Daten. Gegenstand, Art und Zweck sowie Einzelheiten der Datenverarbeitung und der Art der personenbezogenen Daten und Kategorien von Betroffenen richten sich nach den vom Kunden jeweils lizenzierten Adobe Cloud Services und sind in der jeweiligen Dokumentation näher beschrieben. Personenbezogene Daten können die auf der Website des Adobe Privacy Center aufgeführten Kategorien umfassen: www.adobe.com/go/processing.

c) Ein Überblick über die technischen Funktionen von Adobe Creative Cloud sind aufgeführt unter https://www.adobe.com/de/creativecloud/business/enterprise/features.html die der Adobe Document Cloud unter https://acrobat.adobe.com/de/de/acrobat/features.html

Mindestens 30 Tage bevor sich Änderungen am Ort der Verarbeitung oder den Kategorien personenbezogener Daten ergeben wird der Kunde von Adobe in Textform informiert. Nach Ablauf dieser Frist gilt die geänderte Standardweisung. Der Kunde kann sich für individuelle E-Mail-Benachrichtigungen über Updates auf der Website http://www.adobe.com/go/processing anmelden. Der Stand der Verlinkungen zum Vertragsschluss wird als Anlage beigefügt.

4. Verantwortlicher.

In Übereinstimmung mit allen anwendbaren Datenschutzgesetzen ist der Kunde der Verantwortliche und Adobe der Datenverarbeiter soweit dieser alleine oder mit Dritten die Zwecke der Datenverarbeitung ohne Mitwirkung von Adobe festlegt.

5. Betroffene Personen.

Zu den Betroffenen können die Endnutzer des Kunden, Kunden, Interessenten, Geschäftspartner, Lieferanten, Auftragnehmer, Mitarbeiter, Vertreter und Berater gehören.

6. Pflichten von Adobe.

Verarbeitung personenbezogener Daten. Adobe verarbeitet personenbezogene Daten nur im Rahmen der Weisungen des Kunden für den jeweiligen Adobe Cloud Service. Die Standardweisungsmöglichkeiten ergeben sich aus den Standardfunktionalitäten der lizenzierten Produkte und Services. Adobe wird den Kunden unverzüglich informieren, wenn Adobe der Ansicht ist, dass eine Weisung des Kunden gegen Europäische Datenschutzgesetze verstößt, und Adobe ist berechtigt, aber nicht verpflichtet, die Ausführung der betreffenden Anweisung auszusetzen, bis der Kunde diese Anweisung schriftlich

[redacted]

bestätigt. Ungeachtet des Vorstehenden kann Adobe die Personenbezogenen Daten verarbeiten, wenn dies nach dem Recht der Europäischen Union oder des Mitgliedstaates, dem sie unterliegen, erforderlich ist. In diesem Fall wird Adobe den Kunden über eine solche Anforderung informieren, bevor Adobe die Daten verarbeitet, es sei denn, das Gesetz verbietet dies aus wichtigen Gründen des öffentlichen Interesses. Weisungen des Kunden, die über die Standardfunktionen der lizenzierten Produkte und Services hinausgehen, sind vom Kunden zu dokumentieren und deren Ausführung durch Adobe zu protokollieren und von beiden Parteien mindestens drei Jahre lang aufzubewahren. Diese Dokumentation kann auf Anfrage auch nach Vertragsbeendigung gegenseitig eingesehen werden.

7. Sicherheit der Verarbeitung.

a) Adobe hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen die in Anhang 1 beschriebenen technischen und organisatorischen Maßnahmen getroffen und hält diese vor, um ein dem Risiko angemessenes Maß an Sicherheit bei der Verarbeitung Personenbezogener Daten zu gewährleisten. Diese technischen und organisatorischen Maßnahmen wurden Adobe nach Prüfung von unabhängiger Seite zertifiziert. Die Zertifizierungen sind auf der Website des Adobe Trust Center (https://www.adobe.com/security/compliance.html) einsehbar.

b) Adobes technische und organisatorische Maßnahmen werden entsprechend dem technischen Fortschritt weiterentwickelt. Dementsprechend behält sich Adobe das Recht vor, die technischen und organisatorischen Maßnahmen zu ändern, sofern die Funktionalität und Sicherheit der Adobe Cloud Services nicht beeinträchtigt werden und der Schutz der Rechte und Freiheiten der Betroffenen angemessen gewahrt bleibt. Adobe wird durch diese Änderungen das vertraglich vereinbarte Schutzniveau nicht zu Lasten der Betroffenen verändern. Adobe veröffentlicht regelmäßig relevante Informationen über Adobe´s Sicherheitspraktiken: https://www.adobe.com/de/security.html

c) Adobe informiert über Sicherheitsrelevante Ereignisse über diese Webseite: https://helpx.adobe.com/de/security.html

8. Datenschutzverletzung.

Adobe wird dem Kunden eine Datenschutzverletzung unverzüglich, nachdem Adobe von der Datenschutzverletzung Kenntnis erlangt hat über die vom Kunden in Ziffer 17 angegebene E-Mail-Adresse oder wie in der Benutzeroberfläche des Adobe Cloud Services angegeben melden und gemäß Artikel 33 der DSGVO dem Kunden Informationen über die Datenschutzverletzung zur Verfügung stellen (soweit diese Informationen Adobe zur Verfügung stehen), damit der Kunde seinen Meldepflichten gegenüber der Aufsichtsbehörde (und gegebenenfalls den betroffenen Personen) gemäß den Europäischen Datenschutzgesetzen nachkommen kann. Adobe wird unverzüglich eine forensische Untersuchung einer Datenschutzverletzung einleiten und geeignete Abhilfemaßnahmen ergreifen, um mögliche Schäden zu verhindern und zu minimieren. Als zu benachrichtigende Datenschutzverletzungen zählen keine erfolglosen Versuche oder Aktivitäten, welche die Sicherheit Personenbezogener Daten nicht gefährden, einschließlich erfolglose Anmeldeversuche, Denial-of-Service-Angriffe und andere Angriffe auf Firewalls oder vernetzte Systeme.

9. Weitere Verpflichtungen

a) Unter Berücksichtigung der Art der Verarbeitung im Rahmen dieses AV-Vertrags unternimmt Adobe alle angemessenen Maßnahmen, um den Kunden bei der Erfüllung seiner Verpflichtungen gemäß Artikel 30 und 32 bis 36 der DSGVO zu unterstützen.

b) Adobe wird nach Wahl des für die Verarbeitung Verantwortlichen alle Personenbezogenen Daten einschließlich vorhandener Kopien nach Ablauf der geltenden Lizenzvereinbarung löschen oder an den für

[redacted]

die Verarbeitung Verantwortlichen zurückgeben, es sei denn, die Europäischen Datenschutzgesetze verlangen die Speicherung Personenbezogener Daten.

10. Pflichten des Verantwortlichen.

a) Weisungen. Der Kunde kann Adobe die Standardweisungen erteilen, die sich aus dem Lizenzvertrag und den Standardfunktionalitäten ergeben. Für alle hierüber hinausgehenden Weisungen gilt Ziffer 12.

b) Informationspflicht. Wenn der Kunde Kenntnis von Verstößen oder anderen Unregelmäßigkeiten im Zusammenhang mit den anwendbaren Datenschutzgesetzen erlangt, hat er Adobe unverzüglich darüber zu informieren und Weisungen zu erteilen, welche die von Adobe zum Schutz Personenbezogener Daten durchzuführenden Verarbeitungsschritte beschreiben oder die Nichteinhaltung der anwendbaren Datenschutzgesetze zu vermeiden.

11. Aufzeichnungen der Verarbeitung.

Der Kunde ist verpflichtet, jederzeit ein Verzeichnis der unter seiner Verantwortung stehenden Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 1 DSGVO zu führen und auf dem neuesten Stand zu halten.

12. Kosten.

Für den Fall, dass der Kunde Adobe eine Weisung erteilt, deren Ausführung über die Standardfunktionalitäten der Adobe Cloud Services hinausgeht, kann Adobe dem Kunden Kosten in Rechnung stellen, die über die vereinbarten Lizenzgebühren hinausgehen, sofern es für Adobe wirtschaftlich nicht vertretbar ist, diese Weisungen kostenlos auszuführen (unter Berücksichtigung relevanter Faktoren wie Umfang der Anfragen, Komplexität der Weisungen und des angewiesenen Zeitrahmens). Dazu gehören unter anderem die Kosten, die Adobe bei der Ausführung der Weisungen des Kunden in Bezug auf die Löschung, zusätzliche Speicherung und/oder Aufbewahrung der Personenbezogenen Daten des Kunden und die Erfüllung der vom Kunden gemäß Ziffer 13 erhaltenen Zugriffsanfragen entstehen. Adobe wird vor Ausführung einer kostenpflichtigen Weisung den Kunden auf die mögliche Kostenpflicht hinweisen.

13. Zugriff und Datenlöschung.

Anfragen von Betroffenen. Adobe wird den Kunden unverzüglich über alle Anfragen informieren, die Adobe im Zusammenhang mit den vom Kunden lizensierten Adobe Cloud Services erhält. Der Kunde ist dafür verantwortlich, dass solche Anfragen in Übereinstimmung mit den Europäischen Datenschutzgesetzen behandelt werden. Adobe wird geeignete technische und organisatorische Maßnahmen ergreifen, um den Kunden bei seinen Verpflichtungen im Zusammenhang mit derartigen Anfragen zu unterstützen.

14. Audit.

a) Der Kunde kann die Einhaltung der Bestimmungen dieses AV-Vertrages durch Adobe einmal pro Jahr überprüfen (entweder für sich selbst oder im Namen einer Aufsichtsbehörde, der er unterliegt, jedoch nur aufgrund eines formellen Auskunftsersuchens dieser Aufsichtsbehörde) ("Audit").

b) Der Kunde stimmt zu, dass sein oben genanntes Recht auf Audit bedeutet, dass er berechtigt ist, das folgende Verfahren durchzuführen:

i) Der Kunde kann die Ergebnisse der formellen jährlichen unabhängigen Überprüfung der technischen und organisatorischen Maßnahmen ("Compliance-Bericht") überprüfen, die durch einen angesehenen, qualifizierten unabhängigen Dritten durchgeführt wurde.

ii) Soweit der Kunde nach der Prüfung des Compliance-Berichts nicht abgedeckte Bereiche feststellt, die er rechtmäßig nach diesem AV-Vertrag auditieren darf, kann der Kunde Adobe schriftlich eine zusätzliche Liste mit hinreichend spezifischen und detaillierten Fragen vorlegen ("Auditfragen").

[redacted]

(1) Adobe beantwortet die Auditfragen ("Antworten") an den Kunden (oder seine Aufsichtsbehörde, falls vom Kunden angewiesen) innerhalb eines angemessenen Zeitraums.

(2) Mit Erhalt der Antworten auf die Auditfragen ist das Audit des Kunden abgeschlossen, es sei denn, der Kunde kann objektiv nachweisen, dass die Antworten die Einhaltung seiner gesetzlichen Verpflichtungen und dieses AV-Vertrages nicht ausreichend belegen. In einem solchen Fall ist der Kunde berechtigt, sich auf das unten beschriebene Verfahren zu berufen.

iii) Vorbehaltlich der Einhaltung von Unterziffern i. und ii. hat der Kunde das Recht, eine formelle Prüfung der Einhaltung dieses AV-Vertrages durch Adobe in Bezug auf die Prüfungsfragen zu verlangen, die nicht bereits in der von Adobe bereitgestellten Dokumentation enthalten sind ("Gap Audit"). Dazu muss der Kunde Adobe mindestens zwei Wochen vor dem vorgeschlagenen Prüfungstermin einen detaillierten Auditplan vorlegen. Der Auditplan muss den vorgeschlagenen Umfang, die Dauer und das Startdatum des Gap-Audits beschreiben. Adobe prüft den Auditplan und stellt dem Kunden alle Bedenken oder Fragen (z. B. Anfragen nach Informationen, die die Sicherheit, den Datenschutz, die Beschäftigung oder andere relevante Richtlinien von Adobe gefährden könnten), und arbeitet mit dem Kunden zusammen, um einen endgültigen Auditplan zu vereinbaren.

(1) Das Gap-Audit unterliegt den folgenden Bestimmungen:

(a) Das Gap-Audit muss während der normalen Geschäftszeiten des jeweiligen Standorts durchgeführt werden und hat im Einklang mit den Richtlinien von Adobe in Bezug auf Besucher vor Ort an den Standorten zu erfolgen und darf die Geschäftsaktivitäten von Adobe nicht unangemessen beeinträchtigen;

(b) Die Parteien verpflichten sich, die Einhaltung der Verpflichtungen aus diesem AV-Vertrag mit möglichst wenig Störung von Adobe zu überprüfen;

(c) Die Parteien sind sich darüber einig, dass Adobe die Sicherheit seiner Einrichtungen und Standorte und seinen ununterbrochenen Geschäftsbetrieb aufrechterhalten muss, sich selbst und seine Kunden vor Risiken zu schützen hat und die Offenlegung von Informationen, die die Vertraulichkeit von Informationen Adobe´s und seiner Kunden gefährden würden, verhindern muss.

(d) Wenn der Kunde einen Dritten mit der Durchführung des Gap-Audits beauftragt, muss der Dritte in gegenseitigem Einvernehmen zwischen dem Kunden und Adobe eine schriftliche Geheimhaltungsvereinbarung treffen, die für Adobe akzeptabel ist, bevor er das Gap-Audit durchführt.

(e) Wenn der Kunde ein Gap-Audit aufgrund einer Anfrage einer Aufsichtsbehörde durchführt und Adobe und/oder der Unterauftragsverarbeiter der Ansicht ist, dass es nicht möglich ist, einen bestimmten von der Aufsichtsbehörde festgelegten Zeitrahmen einzuhalten, wird Adobe und/oder sein Unterauftragsverarbeiter dem Kunden helfen, dies der zuständigen Aufsichtsbehörde darzulegen. Der Kunde nimmt zur Kenntnis, dass der Zugang zu den Einrichtungen eines Unterauftragsverarbeiters dessen jeweilige Zustimmung bedarf und dass Adobe den Zugang zu den Einrichtungen des Unterauftragsverarbeiters zu einem bestimmten Zeitpunkt nicht gewährleisten kann.

(f) Der Kunde stellt Adobe alle unter diesem Abschnitt erstellten Gap-Audit-Berichte zur Verfügung, sofern dies nicht gesetzlich verboten ist. Der Kunde darf den Gap-Audit-Bericht nur zum Zwecke der Erfüllung seiner behördlichen Prüfungsanforderungen und/oder zur Bestätigung der Einhaltung der Anforderungen dieses AV-Vertrages verwenden.

(g) Der Gap-Audit-Bericht ist eine vertrauliche Information der Parteien gemäß den Bedingungen der Lizenzvereinbarung.

iv) Sofern eine zuständige Aufsichtsbehörde den hier dargestellten Audit als nicht im Einklang mit den geltenden Datenschutzgesetzen befindlich beurteilt, werden weitergehende Rechte des Kunden unter der EU-Datenschutzgrundverordnung nicht eingeschränkt.

15. Unterauftragsverarbeiter.

a) Der Kunde stimmt zu, dass Adobe berechtigt ist, die im Adobe Privacy Center (http://www.adobe.com/go/processing) aufgeführten Unterauftragsverarbeiter für die vom Kunden im Lizenzvertrag erworbenen Adobe Cloud Services zu verwenden. Adobe hat mit dem jeweiligen Unterauftragsverarbeiter Vereinbarungen mit gleichwertigen Verpflichtungen wie in diesem AV-Vertrag vereinbart getroffen. Wenn die Standardvertragsklauseln anwendbar sind und sich der Unterauftragsverarbeiter in einem Drittland befindet, das keinen angemessenen Schutz für Personenbezogene Daten bietet, hat Adobe mit diesem Unterauftragsverarbeiter die Standardvertragsklauseln abgeschlossen. Adobe ist für die Einhaltung der anwendbaren Datenschutzgesetze durch die Unterauftragsverarbeiter gegenüber dem Kunden verantwortlich.

b) Ergänzung weiterer Unterauftragsverarbeiter. Mindestens 30 Tage bevor einem weiteren Unterauftragsverabeiter Zugriff auf Personenbezogene Daten gewährt wird, aktualisiert Adobe die Adobe Processor-Website, was als Benachrichtigung für den Kunden gilt. Der Kunde kann sich für E-Mail-Benachrichtigungen über Updates auf der Adobe Processor-Website anmelden. Will der Kunde der Zustimmung des neuen Unterauftragsverarbeiters widersprechen, so hat er dies Adobe unverzüglich nach Erhalt der Benachrichtigung von Adobe schriftlich mitzuteilen. Widerspricht der Kunde dem neuen Unterauftragsverarbeiter, so kann er den betreffenden Adobe Cloud Service durch schriftliche Kündigung mit Begründung der Nichtzulassung ohne Zahlung einer Vorfälligkeitsentschädigung kündigen.

c) Vereinbarungen mit Unterauftragsverarbeitern. Für den Fall, dass die Standardvertragsklauseln anwendbar sind, vereinbaren die Parteien, dass Kopien von Vereinbarungen mit Unterauftragsverarbeitern, die vom Datenimporteur gemäß Klausel 5 (j) der Standardvertragsklauseln an den Datenexporteur geschickt werden müssen, frei von jeglichen kommerziellen Vereinbarungen sein dürfen und dass diese Vereinbarungen nur auf Anfrage vom Datenimporteur zur Verfügung gestellt werden.

16. Geeignete Garantien für die Übermittlung Personenbezogener Daten in die Vereinigten Staaten von Amerika.

a) EU - U.S. Privacy Shield und Swiss - U.S. Privacy Shield. Adobe Systems Incorporated („Adobe US") ist eine zertifizierte Organisation nach EU - U.S. Privacy Shield und Swiss - U.S. Privacy Shield und beabsichtigt, den Zertifizierungsstatus auch in Zukunft beizubehalten. Für die Übermittlung personenbezogener Daten aus der EU/Schweiz in die USA gelten die Grundsätze des EU - U.S. Privacy Shield und des Swiss - U.S. Privacy Shield Frameworks, es sei denn, der Kunde und Adobe US vereinbaren zu diesem Zweck die Standardvertragsklauseln.

b) Standard-Vertragsklauseln. Wenn sich der Kunde nicht auf die Zertifizierung von Adobe nach dem EU - U.S. Privacy Shield als adäquate Garantie für die Datenübertragung verlassen möchte, schließen der Kunde und Adobe US die Standardvertragsklauseln in Anlage 1 für die Übertragung und Verarbeitung personenbezogener Daten ab.

c) Der Kunde ist zu einer außerordentlichen Kündigung der jeweiligen Lizenzvereinarung berechtigt, wenn der Datentransfer in Drittländer ohne Alternativen seitens Adobe dem Kunden untersagt wird oder rechtlich unzulässig ist, es sei denn ein Übermittlung Personenbezogener Daten in Drittländer ist für die Nutzung der jeweiligen Adobe Cloud Services nicht erforderlich.

17. Kontaktinformationen und Mitteilungen:

Für Adobe:
Bei allgemeinen Fragen mit rechtlichem Bezug: centrallegal@adobe.com

Data Protection Officer

[redacted]

Adobe Systems Software Ireland Limited
4-6 Riverwalk,
City West Business Campus
Dublin 24
Ireland
Email: [redacted]@adobe.com

Das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften kann zudem eine Kontaktperson für Datenschutzfragen bezüglich der Rahmenvereinbarung benennen.

Für den Kunden:

Datenschutzbeauftragter:

[redacted]

Vertreter des Verantwortlichen:

[redacted]

18. Verschiedenes.

Die vom Kunden angegebenen Kontaktinformationen des Datenschutzbeauftragten und des Vertreters des Verantwortlichen werden auch dem Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften offengelegt, um einen Austausch mit der Kontaktperson für Datenschutzfragen des Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften zu ermöglichen, etwa für einen zweiten Informationskanal über anstehende Änderungen der Verarbeitung sowie sicherheitsrelevante Ereignisse. Ergänzungen, Änderungen oder eine Aufhebung dieses AV-Vertrages sind nur in schriftlicher Form zwischen dem Kunden und Adobe und nur mit ausdrücklichem Verweis auf diesen AV-Vertrag gültig. Auf Bitten des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften oder von Adobe kann ein Austausch zu dieser Vereinbarung stattfinden, mit dem Ziel den Vertrag an aktuelle Entwicklungen und Bedürfnisse anzupassen, sofern das bereits vereinbarte Schutzniveau für die Betroffenen nicht unterschritten wird.

[redacted]

Agreement Number: [redacted]

Adobe Systems Software Ireland Limited

Kunde: [redacted]

Unterschrift

Unterschri[redacted]

Name des Unterzeichners

Name des Unterzeichners [redacted]

Datum

Datum [redacted]

[redacted]

07 October 2019 11:53:45 AM

[redacted]

Agreement Number: [redacted]

Technische und Organisatorische Sicherheitsmaßnahmen

I. Sicherheitszertifizierungen von Adobe.

Die Adobe Cloud Services erfüllen die spezifischen Anforderungen des Datenschutzes, einschließlich, aber nicht beschränkt auf Artikel 28 DSGVO und sind gemäß ISO 27001 sowie SOC2, Typ 2 (Security and Availability) zertifiziert, wie hier abrufbar: http://www.adobe.com/go/cloudcompliance

Adobe hat für die die Adobe Cloud Services die im Folgenden beschriebenen technischen und organisatorischen Maßnahmen umgesetzt und unterhält diese Sicherheitsprozesse in den Produktionsumgebungen als Mindeststandard ein:

II. Maßnahmen zur Sicherstellung der Vertraulichkeit

A. Maßnahmen für Betriebsstätten

1. **Zutrittskontrollen**

   a) Der Zutritt zu Betriebsstätten wird Mitarbeitern nach Beendigung des Arbeitsverhältnisses oder nach einem Rollenwechsels, sofern nicht mehr erforderlich, unverzüglich widerrufen. Gegebenenfalls werden temporäre Badges vor dem Verlassen der Betriebsstätte eingezogen.

   b) Genehmigungen für Zutrittsberechtigungen und sämtliche Änderungen an Berechtigungen werden von zuständigen Adobe-Mitarbeitern erteilt.

2. **Überprüfungen von Zutrittsberechtigungen.** Adobe führt quartalsweise Überprüfungen von Zutrittsberechtigungen durch wobei angemessene Korrekturmaßnahmem ergriffen werden.

3. **Gebäudesicherheit**

   a) Der physische Zugang zu den eingeschränkten Bereichen der Betriebsstätten wird durch Wände mit nicht abgetrennten Decken, gesicherten Zugangspforten und/oder personenbesetzten Rezeptionen gesichert.

   b) In allen Betriebsstätten ist der Zugang durch Firmenausweis und/oder biometrische Zugangseinrichtungen gesichert und es werden rund um die Uhr an sieben Tagen die Woche Wachposten eingesetzt. Einige Einrichtungen setzen zusätzliche Maßnahmen (Personenschleusen) ein um zu verhindern, dass Unbefugte Personen unbemerkt den autorisierten Personen in die Betriebsstätte folgen.

   c) In allen Betriebsstätten sind Einbruchmeldeanlagen und Videoüberwachung installiert. Adobe kann die Videoprotokolle nach Bedarf auswerten um Zugänge zu ermitteln.

   d) Die Strom- und Telekommunikationsleitungen von Adobe sind vor Interferenzen, Abhörmaßnahmen geschützt und gegen Beschädigungen gesichert.

   e) Die Erteilung einer Zutrittsberechtigung zu einem Adobe-Datenzentrum bedarf der Genehmigung durch das Management und der dokumentierten Spezifizierung der folgenden Parameter:

      (1) Art des Zutrittsaccounts: (Besucher, Dienstleister, regelmäßig);
      (2) Zugangsberechtigungen, die gewährt werden;
      (3) bestimmungsgemäßer Geschäftszweck;

[redacted]

(4) Maßnahmen zur Identifizierung des Besuchers, soweit angemessen;
(5) Temporärer elektromagnetischer Personenausweis, soweit angemessen;
(6) Beginn der Zugangsberechtigung, und
(7) Dauer des Zugangs.

f) Besucher einer Betriebsstätte zu jeder Zeit begleitet; Zutritt zu den abgetrennten Serverregalen ist verboten.

g) Besucherzugangsprotokolle werden in Übereinstimmung mit den Richtlinien von Adobe zur Aufbewahrung von Dokumenten aufbewahrt.

B. Identitäts- und Zugriffsmanagement von Adobe-Personal.

1. **Logischer Zugriff.**

a) Die Bereitstellung von logischen Zugängen zu Informationssystemen bedarf der Zustimmung des zuständigen Personals.

b) Im Falle der Beendigung des Beschäftigungsverhätnisses werden logische Zugänge widerrufen, entsprechend protokolliert und dem Personalmanagement mitgeteilt.

c) Adobe führt vierteljährlich Kontoüberprüfungen und Zugriffsüberprüfungen durch, und es werden gegebenenfalls Korrekturmaßnahmen ergriffen.

2. **Authentifizierungen.**

a) Adobe erstellt eindeutige Identifikatoren für Benutzerkonten und verhindert die Wiederverwendung von Identitätsmerkmalen. Die Parameter für die Kontoanmeldung folgen diesen Vorgaben:

(1) Die Konten werden nicht geteilt;
(2) Inaktive Sitzungen sind nach 15 Minuten passwortgeschützt; und
(3) Die Konten werden nach 5 fehlgeschlagenen Anmeldeversuchen gesperrt.

b) Die Authentifizierung von Benutzern und Geräten für den Zugang zu Informationssysteme ist durch Passwörter geschützt, die den Vorgaben von Adobe an die Passwortkomplexität genügen. Starke Passwort-Konfigurationen folgen diesen Vorgaben:

(1) Mindestlänge von acht (8) Zeichen;
(2) Kombination von mindestens einem Symbol-/Nummernzeichen zwischen dem ersten und dem letzten Zeichen;
(3) Mindestens ein Alphazeichen;
(4) Nicht auffindbar in einem englischen Wörterbuch;
(5) Keine Wiederholung von drei aufeinanderfolgenden Zeichen des Nutzernamens;
(6) Muss sich von den vorhergehenden zehn (10) Passwörtern unterscheiden.

c) Passwörter für Adobe Informationssystem müssen mindestens alle 180 Tage erneuert werden.

d) Remote Verbindungen in Adobe Netzwerke erfolgt per VPN über kontrollierte Gateways.

3. **Rollenbasierte Zugriffskontrollen.**

a) Erstmalig genehmigte Berechtigungen und Änderungen an Berechtigungen im Zusammenhang mit benutzerdefinierten Zugriffsrollen werden von zuständigem Personal

genehmigt.

b) Der Zugang, der die Änderung von Quellcodes ermöglicht, ist auf autorisiertes Personal beschränkt.

c) Adobe schränkt die Verwendung von Anmeldeinformationen für Sammel- und Gruppenauthentifizierung mit gemeinsam genutzten Verschlüsselungen ein. Die Authentifizierungs-Anmeldeinformationen für Sammel- und und Gruppenkonten werden alle 90 Tage zurückgesetzt.

4. **Netzwerkbetriebsprozesse**

a) Adobe unterhält ein dediziertes Netzwerkbetriebszentrum (Network Operations Center, NOC), das rund um die Uhr mit mindestens zwei dedizierten Mitarbeitern besetzt ist.

b) Netzwerkverkehr zu und von ungeprüften Netzwerken verläuft durch einen Policy Enforcement Point, Firewall-Vorschriften werden in Übereinstimmung mit den identifizierten Sicherheitsanforderungen und erforderlichen Geschäftszwecken festgelegt.

c) Adobe verwendet IDSs, Firewalls und Bastions-Hosts - Access DMZ als Sicherheitsstufen. Antivirensoftware läuft auf allen Desktop- und Laptopcomputern der Mitarbeiter und der gesamte E-Mail-Verkehr wird auf Malware hin überprüft. Darüber hinaus ist On-Demand-Antivirenüberprüfung aktiviert.

d) Die Produktionsumgebungen sind logisch von den Nicht-Produktionsumgebungen getrennt.

5. **Verschlüsselungsprozesse.**

a) Zugang zu den kryptographischen Schlüsselspeichern ist auf autorisiertes Personal beschränkt.

C. Management von Adobe Personal.

1. **Background Checks und Vertraulichkeitsvereinbarungen**

a) Adobe führt Background Checks vor der Einstellung von Personal durch die für der Dauer Beschäftigung vorgehalten werden. Die spezifische Art und der Umfang des Bachgroundheck Berichte, die Adobe typischerweise (je nach anwendbarem Recht) verlangt, kann Folgendes umfassen:

(1) Überprüfung der Bildungsabschlüsse;
(2) Überprüfung vorheriger Anstellungen;
(3) Polizeiliches Führungszeugnis (soweit erlaubt), und,
(4) Überprüfung der angegeben fachlichen und persönlichen Referenzen.

b) Adobe stellt Mitarbeiter auf der Grundlage einer dokumentierten Stellenbeschreibung ein.

c) Mitarbeiter sind verpflichtet, eine Vertraulichkeitsvereinbarung vor Beginn des Beschäftigungsverhältnisses zu unterzeichnen. Adobe Mitarbeiter und Zeitpersonal müssen eine Vereinbarung über den Schutz vertraulicher Informationen unterzeichnen. Die Vertraulichkeitsvereinbarungen gelten auch nach Beendigung des Beschäftigungsverhältnisses weiter.

Zur Klarstellung, Mitarbeiter im Rahmen dieser Ziffer C 1. sind alle Personen, die von Adobe mit der Verarbeitung personenbezogener Daten betraut sind.

2. **Schulungen und Informationsvermittlung**

a) Adobe Mitarbeiter, einschließlich von Zeitpersonal absolvieren Sicherheitstrainings, die jährliche Aktualisierungen über relevante Richtlinien, Normen und neue oder geänderte Angriffsvektoren enthalten, sowie Schulungen für die Meldung sicherheitsrelevanter Ereignisse an die zuständigen Einsatzstellen. Teilnahme und Bestehen der jährlichen Schulungen werden dokumentiert und archiviert.

b) Vollzeitbeschäftigte und Aushilfskräfte von Adobe sowie Praktikanten absolvieren jährliche Schulung über Adobe´s Code of Business Standards. Bei Verstößen gegen den Code of Business Conduct oder andere Richtlinien von Adobe können Disziplinarmaßnahmen bis hin zur Kündigung des Arbeitsverhältnisses oder des Arbeitsvertrags eingeleitet werden.

c) Die von Adobe bestellten Datenschutzbeauftragten und Informationssicherheitsbeauftragten haben die erforderlichen Qualifikation und notwendigen Kompetenzen sowie Ressourcen.

d) Adobe schult und sensibilisiert seine Führungsebene und seine Beschäftigten in Datenschutz und Informationssicherheit.

III. Maßnahmen zur Integrität, Verfügbarkeit und Belastbarkeit von Datenverarbeitungssystemen.

A. Datenverarbeitungssysteme und Technologie Management

1. **Produktions-Konfigurationsmanagement**

a) Adobe stellt sicher, dass die Sicherheitsvorkehrungen und die Basiskonfigurationsnormen gemäß den Industriestandards festgelegt wurden und regelmäßig überprüft und aktualisiert werden.

b) Adobe verwendet Erkennungsmechanismen, um Abweichungen von den Basiskonfigurationen in Produktionsumgebungen zu erkennen.

c) Die Installation von Software oder Programmen in der Produktionsumgebung bedarf der Zustimmung von autorisiertem Fachpersonal.

2. **Change Management**

a) Umfang und Art von Changes sowie die Rollen und Verantwortlichkeiten sind in einem Change-Control-Workflow vorab festgelegt und protokolliert. Darüber hinaus sind die Melde- und Genehmigungspflichten auf der Grundlage des mit demUmfang und der Art der Changes verbundenen Risikos vorab festgelegt.

b) Basierend auf dem Risiko ist vor der Einführung von Changes in einer Produktionsumgebung die Zustimmung von autorisiertem Personal erforderlich, wie nachfolgend beschrieben:

(1) Die Beschreibung des Changes wird protokolliert;
(2) Auswirkungen des Changes;
(3) Die Testergebnisse werden dokumentiert; und,
(4) Es werden Back-Out-Maßnahmen definiert

c) Changes in einer Produktionsumgebung dürfen nur von autorisiertem Personal implementiert werden.

3. **Datenübetragungen**

a) Die Datenkommunikation zwischen den Adobe Standorten zu den Rechenzentren erfolgt über gesicherte dedizierte Netzwerkverbindungen, um die sichere Wartung der Server zu gewährleisten;

b) Alle Netzwerkverbindungen zu den Servern erfolgen über verschlüsselte Secure Shell (SSH), Transport Layer Security (TLS) oder Virtual Private Network (VPN) Kanäle für Fernzugriff und erfordern eine Zwei-Faktor-Authentifizierung;

c) Sofern die Verbindung nicht aus einer Liste von geprüften und genehmigten IP-Adressen stammt, werden Verbindungsversuche von allem anderen IP-Adressen geblockt;

d) Die Übertragung von Daten über das Internet erfolgt verschlüsselt mittels TLS über HTTPS zwischen dem Kunden und der Benutzeroberfläche.

4. **Sicherheitsrichtlinien**

a) Geschäftsunterlagen. Die wichtigsten Geschäftsfunktionen und Informationssicherheitsfunktionen von Adobe werden durch dokumentierte Verfahrensanweisungen vorgegeben, die dem autorisierten Personal mitgeteilt werden.

b) Sicherheitsmanagement & Rollen. Die Rollen und Verantwortlichkeiten für die Governance der Informationssicherheit innerhalb von Adobe werden vom Management formell dokumentiert und kommuniziert.

5. **Monitoring der Cloud Services Systeme**

a) Dokumentation wichtiger Ereigniss in den Informations Systemen:

(1) Adobe verwendet eine zentralisierte SIEM-Lösung, um protokollierte Ereignisse zu aggregieren und in Verbindung mit anderen zu bringen;

(2) Zum Schutz gegen unbefugte Zugriffe und Änderungen erfasst Adobe Netzwerkprotokolle, Betriebssystemprotokolle, Anwendungsprotokolle und Intrusion Detections-Ereignisse.

(3) Die Benutzeraktivität von Applikationen wird von der Applikation protokolliert.

b) Sicherheitsmonitoring und -auswertung

(1) Adobe legt Warnkriterien für das Sicherheitsmonotoring fest, wie die Warnkriterien gekennzeichnet werden und identifiziert autorisiertes Personal für die markierten Systemwarnmeldungen.
(2) Adobe definiert Warnkriterien für das Verfügbarkeitsmonitoring, wie Warnkriterien gekennzeichnet werden und identifiziert autorisiertes Personal für vorgemerkte Systemwarnungen.

c) Dokumentation von Systemdesign

(1) Die Dokumentation der Systemgrenzen und der wichtigsten Komponenten ihrer Funktionalität wird autorisierten Adobe-Mitarbeitern zur Verfügung gestellt.
(2) Adobe veröffentlicht öffentlich zugängliche Whitepapers, in denen der Zweck, die Konzeption und die Grenzwerte der vorgehaltenen Systeme und der jeweiligen Systemkomponenten beschrieben werden, die hier abrufbarsind: https://www.adobe.com/security/resources.html

B. Service & Produkt Lifecycle

1. Quellcode. Quellcode wird mit Hilfe von statischen Codeanalysetools auf Schwachstellen hin überprüft, bevor er in die Produktion freigegeben wird.

2. Software Haupt(Major)-Releases unterliegen dem Service Life-Cycle, der vor der

[redacted]

Implementierung eine Abnahme über die Phasen Konzeptabnahme und Projektplan-Commit voraussetzt.

C. Vulnerability Management

1. Informations Systeme and Technologie

a) Adobe führt Sicherheitsrisikoanalysen durch, ordnet den entdeckten Sicherheitsrisiken Risikobewertungen zu und überprüft tatsächliche Sicherheitsrisiken durch Korrekturen. Die Scan-Tools werden vor der Ausführung von Scans aktualisiert.

b) Mindestens einmal jährlich wird Adobe mit Dienstleistern zusammenarbeiten, um Penetrationstests durchzuführen, entdeckten Sicherheitsrisiken Risikobewertungen zuzuordnen und Sicherheitsrisiken durch Problemlösung zu erfassen.

c) Soweit erforderlich, hat Adobe Enterprise-geeignete Antivirenprogrammen implementiert und stellt Folgendes sicher:

(1) Die Definitionen der Signaturen werden aktualisiert;
(2) Vollständige Scans werden regelmäßig durchgeführt und Echtzeit-Scans sind aktiviert; und
(3) Sicherheitswarnungen werden von autorisiertem Personal überprüft und behoben.

2. Patch Management. Adobe installiert sicherheitsrelevante Patches, einschließlich Software- oder Firmware-Updates, in Übereinstimmung mit dem Patch-Management-Standard von Adobe.

3. Überprüfungen der Sicherheitsrisiken. Adobe prüft Anfragen zu berechtigten Kundenanfragen im Zusammenhang mit Sicherheitsrisiken.

IV. **Maßnahmen zur sofortigen Wiederherstellung und zum Verfügbarkeit von personenbezogenen Daten**

A. **Reaktionen für Störfalle.** Adobe hat ein detailliertes Programm zur Reaktion auf Vorfälle implementiert, das mindestens die folgenden Maßnahmen umfasst, wie auch auf der Website des Adobe Trust Center website beschrieben (https://www.adobe.com/de/security/incident-response.html)

1. Adobe legt die Arten von Ereignissen fest, die bearbeitet, protokolliert und gemeldet werden müssen. Dieses Management umfasst die folgenden Maßnahmen:

a) Maßnahmen für die Identifizierung und Bewältigung von Ereignissen;
b) Maßnahmen zur Behebung von bestätigten Ereignissen;
c) Wichtige Systeme zur Reaktion auf Ereignisse;
d) Maßnahmen für die Identifizierung und Steuerung von Ereignissen;
e) Zentrale Systeme zur Reaktion auf Ereignisse;
f) Koordination und Kommunikationsstrategie von Ereignissen;
g) Kontaktmethode für interne Stellen, um potenzielle Zwischenfälle zu melden;
h) Kontaktdaten des Support-Teams;
i) Meldung an das zuständige Adobe-Management im Falle einer Verletzung des Schutzes von personenbezogenen Daten;
j) Maßnahmen zur Aktualisierung und Kommunikation des Plans;
k) Maßnahmen zur Schulung des Support-Teams;
l) Archivierung von Ereignisinformationen; und,

[redacted]

m) Überprüfung und Genehmigung durch das Management (entweder jährlich oder bei größeren Änderungen der internen Organisation).

2. Adobe reagiert auf bestätigte Ereignisse und die Berarbeitung wird über angemessene Managementkanäle verfolgt. Gegebenenfalls koordiniert Adobe die Reaktion auf Ereignisse mit Maßnahmen für den Notfall.

3. Adobe ermöglicht externen Parteien die Meldung von Vorfällen über eine Kontaktmethode über Adobe´s Incident Response Webseite: https://www.adobe.com/de/security/incident-response.html

C. Maßnahmen zur Abwehr von Umweltgefahren

1. Temperatur- und Luftfeuchtigkeitswerte in den Rechenzentren werden überwacht und auf einem angemessenen Niveau gehalten

2. Die Notfalldienste werden bei der Aktivierung von Brandmeldeanlagen automatisch kontaktiert. Die Konstruktion und Funktion von Brandmelde- und Löschsystemen wird in angemessenen Abständen zertifiziert.

3. Die Konstruktion und Funktion der betreffenden Geräte wird in angemessenen Abständen zertifiziert.

D. Notfall-Wiederherstellung und Business Continuity Pläne

1. Adobe hält Pläne und Prozesse für Disaster Recovery und Business Continuity ein, um die Aufrechterhaltung der Dienste zu ermöglichen und eine wirksame und zuverlässige Wiederherstellung zu gewährleisten. [Beispiel: Sicherungskopien der Datenbände werden durch folgende Verfahren erstellt: Festlegung der Zeitabstände, Speichermedien, Aufbewahrungsdauer und Speicherort der Sicherungskopien].

V. Verfahren zur regelmäßigen Prüfung, Bewertung und Auswertung der Wirksamkeit von Sicherheitsmaßnahmen

A. Risiko Management

1. Das Management von Adobe führt jährlich eine Risikobewertung durch. Die Ergebnisse der Risikobewertungen werden überprüft, um die Minderung der identifizierten Risiken zu priorisieren.

2. Das Management bewertet die Konzeption und operative Effizienz der internen Kontrollen anhand des etablierten Kontroll-Frameworks. Korrekturmaßnahmen im Zusammenhang mit festgestellten Mängeln werden bis zur Behebung verfolgt.

3. Adobe legt die Anforderungen an das interne Audit fest und führt in regelmäßigen Abständen Audits an Informationssystemen und Prozessen durch.

4. Das Management erstellt einen Maßnahmenplan, um die Lösung der bei der Risikobewertung festgestellten Mängel formal zu steuern.

B. Management Externer Dienstleister

1. Das Management überprüft regelmäßig die Kontrollmaßnahmen in den Prüfungsberichten Dritter, um sicherzustellen, dass sie den organisatorischen Anforderungen entsprechen. Wenn in den Prüfungsberichten Kontrolllücken festgestellt werden, untersucht das Management die Auswirkungen der offenbarten Lücken für die Sicherheit der Daten.

2. Adobe führt eine Risikobewertung durch, um die Datentypen zu ermitteln, die von einem Managed Service Provider verarbeitet werden können.

Agreement Number: [redacted]

Anlage
Adobe Unterauftragsverarbeiter
(Stand 4. October 2019)

ADOBE PRIVACY CENTER

Sub-Processors | Processing Locations for EMEA | Personal Data Categories

To subscribe to notifications of changes or updates to this page, please enter your information here.

Sub-processors applicable to all Adobe Cloud Services (Experience Cloud, Creative Cloud and General Document Cloud)

Name of Entity	Entity Type	Service Provided	Location
Adobe Inc.	Adobe Affiliate	Hosting and Support Services	United States
Adobe Systems Engineering GmbH	Adobe Affiliate	Support Services	Germany
Adobe Systems India Pvt. Ltd	Adobe Affiliate	Support Services	India
Adobe Systems Romania S.r.l	Adobe Affiliate	Support Services	Romania
Adobe Research Schweiz AG	Adobe Affiliate	Support Services	Switzerland
Adobe Systems Canada, Inc.	Adobe Affiliate	Support Services	Canada
Adobe Systems Europe Limited	Adobe Affiliate	Support Services	United Kingdom
Amazon Web Services Inc and affiliates	Data Center	3rd Party Hosting	United States European Union
Microsoft Azure	Data Center	3rd Party Hosting	United States European Union

Sign In

ADOBE PRIVACY CENTER

Sub-processors specific to Adobe Sign (Electronic Signature Service)

Name of Entity	Entity Type	Service Provided	Location
Amazon Web Services Inc and its affiliates	Data Center	3rd Party Hosting	Germany[1]
j2 Cloud Services, Inc (eFax)	3rd Party Provider		United States
Telesign Corp	3rd Party Provider		United States
Adobe Inc.	Adobe Affiliate	Support Services	United States
Adobe Systems Europe Limited	Adobe Affiliate	Support Services	United Kingdom
Adobe Systems India Pvt Ltd	Adobe Affiliate	Support Services	India
Adobe Systems Romania S.r.l.	Adobe Affiliate	Support Services	Romania

(1) Default location for EMEA-based customers, unless otherwise direct by the customer during provisioning of Adobe Sign services.

f 3 04/10/2019, 16:13

07 October 2019 11:53:45 AM

[redacted]

Agreement Number: [redacted]

Standorte der Datenverarbeitung

ADOBE PRIVACY CENTER

Sub-Processors | **Processing Locations for EMEA** | Personal Data Categories

Adobe Cloud Service	Location of Processing
Adobe Analytics, Adobe Target and Adobe AdCloud	European Union
Adobe Social (other than Social Moderation)	European Union
Adobe Social (Social Moderation)	United States
Adobe Experience Manager Managed Services, Adobe Campaign Managed Services and Adobe Cloud Messaging Services	European Union
IP Obfuscation (Replace Visitors Last IP Octet with 0 setting enabled)	European Union
Audience Manager	United States
Audiences and Profiles	United States
Adobe Connect	European Union
Adobe Creative Cloud, Adobe Document Cloud, Adobe Sign	European Union[1]

[1] User authentication process occurs in the United States

Kategorien Personenbezogener Daten

ADOBE PRIVACY CENTER

Sub-Processors | Processing Locations for EMEA | **Personal Data Categories**

Adobe may process the categories of Personal Data set out in the table below, as determined at the sole discretion of Customer:

Personal Details and contact information	Name
	Address
	Email address
	Title
	Position
	Contact information
	Social profile information
	IP address
	Unique user IDs (such as cookie IDs)
	Marketing profiles
Documents, images and content	Documents uploaded to the Adobe Cloud Services in electronic form which may contain any type of Personal Data
	Images uploaded to the Adobe Cloud Services in electronic form which may contain any type of Personal Data
	Content uploaded to the Adobe Cloud Services in electronic form which may contain any type of Personal Data

07 October 2019 11:53:45 AM

[redacted]

Agreement Number: [redacted]

Standardvertragsklauseln (Auftragsdatenverarbeiter)

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

Die Gesellschaft, die auf dem Bestelldokument und der Auftragsdatenvereinbarung für die Adobe Cloud Services (mit den EU Standardvertragsklauseln, zu welchen diese Standardvertragsklauseln angehängt sind) als „Kunde" bezeichnet ist

("Datenexporteur")

und

Adobe Inc.

345 Park Avenue, San Jose, CA95110

("Datenimporteur")

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

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

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke *„personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle"* entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

b) der *„Datenexporteur"* ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der *„Datenimporteur"* ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Weisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der *„Unterauftragsverarbeiter"* ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Weisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff *„anwendbares Datenschutzrecht"* bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die *„technischen und organisatorischen Sicherheitsmaßnahmen"* sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

[redacted]

07 October 2019 11:53:45 AM

Klausel 2

Einzelheiten der Übermittlung

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

Klausel 3

Drittbegünstigtenklausel

1. Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

2. Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

3. Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

4. Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

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

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Weisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

1. Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

2. Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

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

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

Klausel 7

Schlichtungsverfahren und Gerichtsstand

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

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

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

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

Klausel 8

Zusammenarbeit mit Kontrollstellen

1. Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrages bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

2. Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

3. Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaates, in dem der Datenexporteur niedergelassen ist, nämlich: Deutschland

Klausel 10

Änderung des Vertrags

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

Klausel 11

Vergabe eines Unterauftrags

1. Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

2. Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

3. Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: Deutschland.

4. Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

1. Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

2. Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Für den Datenexporteur

[redacted]

Für den Datenimporteur

_____
Unterschrift

_____
Name (ausgeschrieben)

_____
Funktion

_____
Anschrift

[redacted]

Agreement Number: [redacted]

Anhang 1 zu den Standardvertragsklauseln

Datenexporteur

Der Datenexporteur ist in der Lizenzvereinbarung, zu dem diese Standardvertragsklauseln angehängt sind, als "Kunde" bezeichnet. Der Kunde hat die in der Lizenzvereinbarung angegebenen Adobe Cloud Services lizenziert.

Datenimporteur

Der Datenimporteur ist Adobe Systems Incorporated, ein Lieferant von Software und Services für den Datenexporteur.

Betroffene Personen

Betroffene Personen können die Endkunden, Kunden, potenziellen Kunden, Geschäftspartner Lieferanten, Auftragnehmer, Arbeitnehmer, Erfüllungsgehilfen und Berater des Datenexporteurs sein.

Kategorien von Daten

Die Kategorien von personenbezogenen Daten, die der Datenimporteur verarbeiten kann sind die auf der Website des Adobe Privacy Centers aufgeführt: www.adobe.com/go/processing

Besondere Arten von personenbezogenen Daten

Die übertragenen personenbezogenen Daten können – nach freiem Ermessen des Datenexporteurs und wie gemäß der Lizenzvereibarung gestattet – die folgenden Kategorien von besonderen personenbezogenen Daten enthalten:

- Sexuelle Präferenzen
- Medizinische oder Gesundheitsinformationen
- Politische oder philosophische Meinungen
- Religiöse Überzeugungen
- Gewerkschaftszugehörigkeit
- Rassische und ethnische Herkunft

Zweck der Übermittlung / Verarbeitungsvorgänge

Die übertragenen personenbezogenen Daten werden wie folgt verarbeitet:

Die Verarbeitung personenbezogener Daten durch den Datenimporteur erfolgt, um (1) die Adobe Cloud Services zu erbringen; (2) vom Datenexporteur verlangten technischen und Kunden-Support zu erbringen; und (3) alle anderen Pflichten gemäß der Lizenzvereinbarung zu erfüllen.

[redacted]

Agreement Number: [redacted]

Anhang 2 zu den Standardvertragsklauseln

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

Der Datenimporteur hat die technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten vor Missbrauch und zufälliger Zerstörung und Verlust, wie in Klausel 4.4 und Anlage 2 der Vereinbarung über Auftragsverarbeitung für Adobe Cloud Services (mit EU Standardvertragsklauseln) beschrieben, eingeführt und wird diese beibehalten. Durch diese Bezugnahme sind diese Maßnahmen in diesen Anhang 2 einbezogen.

[redacted]