HQ (Americas / APJ)
119 5th Ave, 7th Floor | New York, NY 10003 | USA
+1 630 974 3000

HQ (EMEA)
Torsgatan 11 | Box 7007 | 103 86 Stockholm | Sweden
Reg. #: 556208-3435
+46 8 55 58 27 00

Datenverarbeitungsvertrag (DPA)

Anlage 3 zum MSA (DSGVO, Standardvertragsklauseln (2021), Verbindliche Unternehmensregeln für die Gesellschaft als Auftragsverarbeiter)

Aktualisierung von 17. Juli 2021

EINLEITUNG

Der Auftragsvereinbarungsvertrag („AVV“ oder „Data Processing Agreement („**DPA**”)) ist Teil des Master Services Agreements, einschließlich aller Bestellungen, Anlagen und Dokumente, auf die Bezug genommen wird, oder anderer schriftlicher bzw. elektronischer Vereinbarungen zwischen Gesellschaft und Kunden zum Erwerb von Online-Services von der Gesellschaft (im entsprechenden Vertrag entweder als „**Software Services**” oder anderweitig benannt und nachfolgend als „**Software Services**” bezeichnet) („**Vertrag**”). Er beinhaltet die Übereinkunft der Vertragsparteien bezüglich der Verarbeitung personenbezogener Daten.

Der Kunde unterzeichnet diesen Vertrag in eigenem Namen sowie, im von den geltenden Datenschutzgesetzen und -verordnungen vorgesehenen Umfang, im Namen seiner autorisierten verbundenen Unternehmen, falls und soweit die Gesellschaft personenbezogene Daten für diese autorisierten verbundenen Unternehmen als Datenverantwortliche verarbeitet. Für die Zwecke dieses DPAs umfasst der Begriff „**Kunde**“, falls nicht anderweitig angegeben, den Kunden und dessen autorisierte verbundene Unternehmen. Alle Fachbegriffe, die in diesem Datenverarbeitungsvertrag nicht definiert sind, besitzen die im Vertrag („**MSA**“), im End-User Services Agreement („**EUSA**“) und im Service Level Agreement („**SLA**“) erläuterten Bedeutungen.

Im Zuge der Bereitstellung der Software Services an den Kunden gemäß dem Vertrag kann die Gesellschaft personenbezogene Daten für den Kunden verarbeiten und die Parteien vereinbaren in Bezug auf alle personenbezogenen Daten die Einhaltung der im Folgenden genannten Bestimmungen. Sie handeln dabei angemessen und in gutem Glauben.

UNTERZEICHNUNG DIESES DPAs:

1. Dieser DPA besteht aus zwei Teilen: dem Hauptvertragstext sowie den Anhängen 1 (einschließlich Anlage), 2 und 3.
2. Sind dieser DPA Verträge oder Bestellungen beigefügt, die unterzeichnet sind, sind sie als Teil des Vertrags oder der Bestellung zwischen den Parteien rechtlich bindend.
3. Ist dieser DPA keinem Vertrag oder Bestellung beigefügt, wurde er vorab im Namen der Gesellschaft unterzeichnet und der Kunde handelt entsprechend Schritt 4. Die Standardvertragsklauseln in Anhang 1 wurden vorab im Namen der Gesellschaft als Datenimporteur unterzeichnet.
4. Um diesen DPA auszufüllen, wenn er nicht einem Vertrag oder einer Bestellung beigefügt ist, geht der Kunde wie folgt vor:
    a. Er füllt die Informationen im Unterschriftenfeld aus und unterzeichnet auf Seite 7.
    b. Er beachtet auf Seite 16, dass unterschiedliche Unterauftragsverarbeiter für unterschiedliche Services eingesetzt werden.
    c. Er übermittelt den ausgefüllten und unterzeichneten DPA per E-Mail oder Webformular unter Angabe seines Account-Namens (aus Vertrag, Bestellung oder Rechnung entsprechend ersichtlich) an die Gesellschaft, und zwar an privacy@optimizely.com. Sobald die Gesellschaft den korrekt ausgefüllten und unterzeichneten DPA unter dieser E-Mail-Adresse oder über das Webformular erhält, wird dieser DPA rechtlich bindend.

GELTUNGSBEREICH DIESES DPAs

Ist der Kunde, der diesen DPA unterzeichnet, eine Vertragspartei, dann bildet dieser DPA einen Teil des Vertrags. In diesem Fall ist das Unternehmen der Gesellschaft, das Vertragspartei ist, Vertragspartner dieses DPAs.

Unterzeichnet ein verbundenes Unternehmen des Kunden diesen DPA und hat im Rahmen des Vertrags eine Bestellung bei der Gesellschaft oder dessen verbundenem Unternehmen abgeschlossen, ist jedoch selbst nicht Vertragspartei, dann gilt dieser DPA als dieser Bestellung und den zugehörigen neuerlichen Bestellungen beigefügt und das Unternehmen der Gesellschaft, das Vertragspartei der Bestellung ist, ist auch Partei dieses DPAs.

Ist das Unternehmen des Kunden, das diesen DPA unterzeichnet, nicht direkt mit der Gesellschaft Vertragspartei einer Bestellung oder eines Master Services Agreements, sondern indirekt über einen autorisierten Reseller der Dienstleistungen der Gesellschaft, dann ist dieser DPA ungültig und nicht rechtsverbindlich. Das Unternehmen sollte in diesem Fall den autorisierten Reseller kontaktieren, um zu erörtern, ob eine Ergänzung seines Vertrags mit dem Reseller erforderlich ist.

Dieser DPA ersetzt nicht zusätzliche Bestimmungen bezüglich der Verarbeitung von Kundendaten, die in Vertragsergänzungen des Kunden enthalten sind, ersetzt jedoch bereits vorhandene Datenverarbeitungsverträge zwischen den Parteien.

Unterzeichnet ein Unternehmen, das nicht Partei eines Vertrags oder einer Bestellung ist, diesen DPA, dann ist dieser DPA ungültig und nicht rechtsverbindlich. Das Unternehmen sollte in diesem Fall ein Unternehmen des Kunden, das Partei des Vertrags ist, auffordern, diesen DPA in seinem Namen zu unterzeichnen.

**Hinweis: Nutzt der Kunde Episerver Managed Services (vormals Everweb oder Ektron Holding), ist dieser DPA nicht gültig und nicht rechtsverbindlich, wenn nicht eine schriftliche Bestätigung der Gesellschaft vorliegt, dass die Umgebung des Kunden die Mindestanforderungen der DSGVO bezüglich technischer und organisatorischer Sicherheitsmaßahmen erfüllt.*

Begriffe des DPAs

1. Definitionen

1.1. **„Verbundenes Unternehmen"** ist jedes Unternehmen, das die Kontrolle über eine der Vertragsparteien hat, von einer der Vertragsparteien kontrolliert wird oder unter ihrem beherrschendem Einfluss steht. Der Begriff **„Kontrolle"** bezieht sich auf die Macht oder Befugnis, auf die Geschäftstätigkeit des Unternehmens durch Halten einer Mehrheit der stimmberechtigten Aktien direkt Einfluss zu nehmen. In Bezug auf die Gesellschaft bezieht er sich auf das Unternehmen von Episerver, das Partei dieses Vertrags ist bzw. eine Bestellung oder ein anderes Dokument als Teil des Vertrags unterzeichnet. Dazu zählen Optimizely Inc. mit Sitz in Delaware, USA, Episerver Inc. mit Sitz in Delaware, USA, Episerver AB mit Sitz in Schweden, Episerver UK Ltd. mit Sitz in England und Wales sowie Episerver GmbH mit Sitz in Berlin, Deutschland.

1.2. **„Autorisiertes verbundenes Unternehmen"** ist jedes verbundene Unternehmen des Kunden, das (a) den Datenschutzgesetzen und -verordnungen der Europäischen Union, des Europäischen Wirtschaftsraums und/oder deren Mitgliedstaaten, der Schweiz und/oder des Vereinigten Königreichs unterliegt, und (b) dem es gemäß dem Vertrag zwischen Kunde und Gesellschaft gestattet ist, die Software Services, wie im entsprechenden Bestellformular oder MSA angegeben, zu nutzen.

1.3. **„Gesellschaft"** ist das Unternehmen, das Vertragspartei dieses DPAs ist und Mitglied des Konzerns.

1.4. **„Konzern"** bezeichnet die Gesellschaft und ihre verbundenen Unternehmen, die mit der Verarbeitung personenbezogener Daten befasst sind. Dazu zählen Optimizely Inc. mit Sitz in Delaware, USA, Episerver Inc. mit Sitz in Delaware, USA, Episerver AB mit Sitz in Schweden, Episerver UK Ltd. mit Sitz in England und Wales, Episerver GmbH mit Sitz in Berlin, Deutschland, Episerver Research and Development Company Limited mit Sitz in Vietnam, Episerver Pty Ltd mit Sitz in New South Wales, Australien, Insite Software Solutions Inc. mit Sitz in Delaware, USA, Idio Inc. mit Sitz in Delaware, USA, und Zaius Inc. mit Sitz in Delaware, USA.

1.5. **„Company BCR"** (Binding Corporate Rules der Gesellschaft) sind die verbindlichen Unternehmensregeln für die Verarbeitung personenbezogener Daten. Deren aktuelle Version ist auf der Webseite der Gesellschaft derzeit abrufbar unter: http://www.optimizely.com/trust-center/ und regelt die Übermittlung personenbezogener Daten an Drittstaaten, zwischen Konzernmitgliedern und an Dritte, die als Unterauftragsverarbeiter fungieren. Der Geltungsbereich der Company BCR ist in Abschnitt 8.3 dieses DPA dargelegt.

1.6. **„Verantwortlicher"** ist die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

1.7. **„Kundendaten"** folgt der Definition im Vertrag unter „**Kundendaten**" oder „**Ihre Daten**".

1.8. **„Data Privacy, Protection, Security and Architecture Documentation"** oder **„DPPSAD"** (Dokumentation zu Datenschutz, Sicherheit und Architektur) ist die Dokumentation zu Datenschutz, Sicherheit und Architektur, die dem Kunden für seine erworbenen Software Services zur Verfügung steht. Diese wird von Zeit zu Zeit aktualisiert und ist in den Standardvertragsklauseln Anlagen 1 und 2 oder über das Trust Center der Gesellschaft, https://www.optimizely.com/trust-center/ bzw. Optimizely World https://world.optimizely.com/ zu finden. Gegebenenfalls wird sie auf andere angemessene Weise durch die Gesellschaft bereitgestellt.

1.9. **„Datenschutzgesetze und -verordnungen"** sind alle Rechtsvorschriften und Verordnungen, die bei der Verarbeitung von personenbezogenen Daten im Rahmen des Vertrags einzuhalten sind. Dazu gehören unter anderem die Rechtsvorschriften und Verordnungen der Europäischen Union („**EU**"), des Europäischen Wirtschaftsraums („**EWR**") und ihrer Mitgliedstaaten, der Schweiz und des Vereinigten Königreichs.

1.10. **„Betroffene Person"** ist die identifizierte oder identifizierbare Person, zu der die personenbezogenen Daten gehören.

1.11. **„DSGVO"** steht für (i) die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) und (ii) im Zusammenhang mit der Verarbeitung personenbezogener Daten, bei der die geltenden Datenschutzgesetze und -verordnungen besagen, dass für die Verarbeitung diejenigen des Vereinigten Königreichs gelten, die UK-DSGVO (wie im Data Protection Act 2018 festgelegt).

1.12. **„Geofencing"** besitzt die dem Begriff in Anhang 3 (Ergänzende Maßnahmen) zugewiesene Bedeutung.

1.13. **„Personenbezogene Daten"** sind (i) alle Informationen zu einer identifizierten oder identifizierbaren natürlichen Person und/oder (ii) alle Informationen, die anderweitig als personenbezogene Daten, personenbezogene Informationen, zu einer Person zuzuordnende Informationen (oder ähnliches) gemäß der geltenden Datenschutzgesetze und -verordnungen geschützt sind und bei denen es sich sowohl bei (i) als auch bei (ii) um Kundendaten handelt.

1.14. **„Verarbeitung"** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.15. **„Auftragsverarbeiter"** ist eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.16. **„Standardvertragsklauseln"** oder **„SCCs"** (Standard Contractual Clauses) bezieht sich auf den zwischen Kunde und Gesellschaft unterzeichneten und diesem Dokument als Anhang 1 beigefügten Vertrag gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer, die kein angemessenes Datenschutzniveau sicherstellen, sowie auf alle Verträge zwischen Kunde und Gesellschaft gemäß Anhang 3 (Ergänzende Maßnahmen), die diesen zu gegebener Zeit ersetzen. Handelt es sich bei den geltenden Datenschutzgesetzen und -verordnungen um die Rechtsvorschriften und Verordnungen des Vereinigten Königreiches, ist „Standardvertragsklauseln" oder „SCCs" als Standarddatenschutzklauseln nach Maßgabe des Art. 46 UK-DSGVO zu verstehen.

1.17. **„Unterauftragsverarbeiter"** ist ein von der Gesellschaft oder einem Mitglied des Konzerns beauftragter Auftragsverarbeiter.

1.18. **„Aufsichtsbehörde"** ist eine unabhängige, gemäß DSGVO errichtete Behörde eines EU-Mitgliedstaats oder eine Regulierungsbehörde gemäß anderer Datenschutzgesetze und -verordnungen.

2. Verarbeitung personenbezogener Daten

2.1. **Einschränkungen bei Software Services**. Die Parteien vereinbaren, dass die von der Gesellschaft bereitgestellten Software Services den Servicebeschreibungen unter https://world.optimizely.com/services/descriptions/ entsprechen. In diesen Servicebeschreibungen ist angegeben, ob ein bestimmter Software Service die Verarbeitung personenbezogener Daten durch den Kunden gestattet oder nicht. Ist in einer Servicebeschreibung angegeben, dass ein bestimmter Software Service die Verarbeitung personenbezogener Daten durch den Kunden nicht gestattet (oder die Servicebeschreibung eine eingeschränkte Verarbeitung personenbezogener Daten vorgibt, zum Beispiel unter der Voraussetzung des Geofencings), dann gilt für den Kunden:

2.1.1. (wenn die Servicebeschreibung eines Software Services die Verarbeitung personenbezogener Daten durch den Kunden nicht gestattet), dass er keine personenbezogenen Daten im Rahmen des betreffenden Software Services verarbeitet, und/oder

2.1.2. (wenn die Servicebeschreibung eines Software Services die eingeschränkte Verarbeitung personenbezogener Daten gestattet), dass er keine personenbezogenen Daten im Rahmen des betreffenden Software Services verarbeitet, ohne die diesbezügliche Einschränkung einzuhalten.

Ohne die schriftliche anderweitige Zustimmung der Gesellschaft hat der Kunde die oben genannten Einschränkungen der Verarbeitung in jedem Fall zu beachten. Der vorliegende Abschnitt 2.1 besitzt Vorrang vor allen anderen gegenteiligen Bestimmungen dieser DPA und Bezugnahmen auf personenbezogene Daten und Verarbeitung im Rest dieses Vertrags sind entsprechend auszulegen.

2.2. **Rollen der Parteien.** Die Parteien vereinbaren in Hinblick auf die Verarbeitung personenbezogener Daten, dass der Kunde als Verantwortlicher und die Gesellschaft als Auftragsverarbeiter fungieren und dass die Gesellschaft oder Mitglieder des Konzerns Unterauftragsverarbeiter gemäß den Anforderungen in Annex III der Anlage zu Anhang 1 („**Unterauftragsverarbeiter**") unten beauftragt bzw. beauftragen.

2.3. **Verarbeitung personenbezogener Daten durch die Gesellschaft.** Die Gesellschaft behandelt personenbezogene Daten als vertrauliche Informationen und verarbeitet personenbezogene Daten nur in Einklang mit den dokumentierten Weisungen des Kunden zu den folgenden Zwecken: (i) Verarbeitung gemäß dem Vertrag und der/den zugehörigen Bestellung(en), (ii) Verarbeitung ausgelöst durch Benutzer im Zuge ihrer Nutzung der Software Services und (iii) Verarbeitung gemäß anderer angemessener schriftlicher Weisungen des Kunden (auch per E-Mail), wenn diese Weisungen in Einklang mit den Bestimmungen des Vertrags liegen.

2.4. **Verarbeitung personenbezogener Daten durch den Kunden.** Bei seiner Nutzung der Software Services hat der Kunde personenbezogene Daten in Einklang mit den Anforderungen der Datenschutzgesetze und -verordnungen zu verarbeiten. Zur Klarstellung: Die Weisungen des Kunden zur Verarbeitung personenbezogener Daten müssen mit den Datenschutzgesetzen und -verordnungen in Einklang stehen. Der Kunden trägt die alleinige Verantwortung für

2.4.1. die Richtigkeit, Qualität und Rechtmäßigkeit personenbezogener Daten und die Mittel, mit denen der Kunde personenbezogene Daten erfasst, einschließlich der erforderlichen Mitteilungen und Einwilligungen in Bezug auf diese personenbezogenen Daten.

2.4.2. die Feststellung aller Datenbanken, die personenbezogene Daten enthalten, für welche die Einschränkungen des Geofencings anzuwenden sind, um die Datenschutzgesetze und -verordnungen sowie die Mitteilungspflichten im Rahmen dieser Einschränkungen gemäß Anhang 3 (Ergänzende Maßnahmen) zu erfüllen, und

2.4.3. die Sicherstellung, dass alle Übermittlungen personenbezogener Daten an Dritte (die nicht zum Konzern gehören oder Unterauftragsverarbeiter sind), die entweder (i) über Konten oder Verbindungen, die vom Kunden eingerichtet wurden und bei der Nutzung von Software Services genutzt werden, oder (ii) über Konten oder Verbindungen, die von der Gesellschaft eingerichtet wurden, vollzogen werden, den Datenschutzgesetzen und -verordnungen entsprechen. Dazu gehört gegebenenfalls auch die Sicherstellung der Erfüllung der Anforderungen in den Artikel 44-49 DSGVO. Als Verantwortlicher übernimmt der Kunde die alleinige Verantwortung für (i) die Festlegung, welche personenbezogenen Daten er übermittelt oder die Gesellschaft anweist zu übermitteln, (ii) die Beurteilung, welche Datenschutzgesetze und -verordnungen auf die jeweiligen Übermittlungen anzuwenden sind, und (iii) die Auswahl der Dritten als Übermittlungsempfänger sowie die entsprechenden Vertragsbedingungen (einschließlich der Beurteilung der Notwendigkeit und Angemessenheit ergänzender Garantien, um den Schutz der personenbezogenen Daten in dem Land, in das sie importiert werden, sicherzustellen). Der Kunde erkennt an, dass die Gesellschaft (als Auftragsverarbeiter) in keiner vertraglichen (oder anderen) Beziehung zu genannten Dritten steht, keine Kontroll- oder Aufsichtsbefugnis über sie oder ihre Verarbeitungsvorgänge, die sich bisweilen ändern können, hat und es aus diesem Grund angemessen ist, dass der Kunde allein verantwortlich für die Regelüberwachung ist. Als Verantwortlicher stellt der Kunde fortwährend sicher, dass die Verarbeitung personenbezogener Daten durch Dritte in Einklang mit den geltenden Datenschutzgesetzen und -verordnungen steht, und informiert die Gesellschaft unverzüglich, sollte er davon Kenntnis erlangen, dass eine Übermittlung personenbezogener Daten durch die Gesellschaft nicht länger in Einklang mit den geltenden Datenschutzgesetzen und -verordnungen steht. In diesem Fall ist die Gesellschaft berechtigt, die betreffenden Übermittlungen einzustellen und der Kunde ergreift umgehend die erforderlichen Maßnahmen, um eine solche Nichteinhaltung zu beheben. Ungeachtet der vorgenannten Bestimmungen im vorliegenden Abschnitt 2.4.3 leistet die Gesellschaft auf schriftliche Aufforderung des Kunden hin angemessene Hilfestellung bei der Sicherstellung, dass die Übermittlungen in Einklang mit den Datenschutzgesetzen und -verordnungen stehen.

2.5. **Details der Verarbeitung.** Gegenstand der Verarbeitung personenbezogener Daten durch die Gesellschaft ist die Erbringung der Services gemäß dem Vertrag. Die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen, die im Rahmen dieses DPA verarbeitet werden, sind im Detail in Anhang 2 (Details der Verarbeitung, Kategorien von Daten und betroffenen Personen) zu diesem DPA ausgeführt.

3. Pflichten des Auftragsverarbeiters

3.1. Ressourcen, Personal und Mitarbeiter der Gesellschaft

3.1.1. Geheimhaltung. Die Gesellschaft stellt sicher, dass das Personal, das in die Verarbeitung personenbezogener Daten eingebunden ist, über die Vertraulichkeit der personenbezogenen Daten informiert ist, die entsprechende Schulung zu seinen Verantwortlichkeiten erhalten und Vertraulichkeitsvereinbarungen unterzeichnet hat. Die Gesellschaft gewährleistet, dass diese Geheimhaltungspflichten über die Beendigung von Arbeitsverhältnissen hinaus fortbestehen.

3.1.2. Zuverlässigkeit. Die Gesellschaft unternimmt alle angemessenen Schritte zur Gewährleistung der Zuverlässigkeit des in die Verarbeitung personenbezogener Daten eingebundenen Personals.

3.1.3. Zugangsbeschränkung. Die Gesellschaft stellt sicher, dass der Zugang der Gesellschaft auf personenbezogene Daten auf die Personen beschränkt ist, welche in Einklang mit dem Vertrag Services erbringen.

3.1.4. Datenschutzbeauftragter. Jede Gesellschaft des Konzerns verfügt über einen Datenschutzbeauftragten. Die benannte Person ist unter dpo@optimizely.com zu erreichen.

3.1.5. Gebiet. Der Kunde bestätigt, dass die Gesellschaft, im Sinne dieses DPA und vorbehaltlich

3.1.5.1. etwaiger Einschränkungen bezüglich Geofencing gemäß Anhang 3 (Ergänzende Maßnahmen) sowie

3.1.5.2. bestimmter zusätzlicher zwischen Kunde und Gesellschaft gemäß Anhang 3 (Ergänzende Maßnahmen) vereinbarter Maßnahmen,

berechtigt ist, personenbezogene Daten im Rahmen dieses DPAs in Drittländern außerhalb der EU / des EWRs zu verarbeiten, insbesondere in Vietnam, Australien, den USA und dem Vereinigten Königreich nur zu Zwecken des Supports.

3.2. Sicherheit

3.2.1. Kontrollen zum Schutz von Kundendaten. Die Gesellschaft ergreift angemessene technische und organisatorische Maßnahmen zur Gewährleistung von Sicherheit, Vertraulichkeit und Integrität der Kundendaten, wie in der DPPSAD ausgeführt. Dies umfasst unter anderem –

3.2.1.1. das Verwehren des Zugangs von Unbefugten zu den personenbezogene Daten verarbeitenden Software Services (physische Zugangskontrolle), soweit es dem Auftragsverarbeiter möglich ist,

3.2.1.2. das Verhindern der Nutzung der personenbezogenen Daten verarbeitenden Software Services durch Unbefugte (logische Zugriffskontrolle), soweit es dem Auftragsverarbeiter möglich ist,

3.2.1.3. sicherzustellen, soweit es dem Auftragsverarbeiter möglich ist, dass Personen, die berechtigt sind, personenbezogene Daten verarbeitende Software Services zu nutzen, nur auf diejenigen Daten Zugriff haben,

zu denen sie entsprechend ihrer Zugangsrechte und den Weisungen des Verantwortlichen berechtigt sind, und dass personenbezogene Daten im Zuge ihrer Verarbeitung oder Nutzung und nach ihrer Speicherung nicht ohne Genehmigung gelesen, kopiert, geändert oder gelöscht werden können (Datenzugriffskontrolle),

3.2.1.4. sicherzustellen, soweit es dem Auftragsverarbeiter möglich ist, dass personenbezogene Daten während elektronischer Datenübermittlung, Transport oder Speicherung auf Speichermedien nicht ohne Genehmigung gelesen, kopiert, geändert oder gelöscht werden können und dass die Zielorte einer Übermittlung personenbezogener Daten mithilfe von Datenübertragung bekannt und verifizierbar sind (Datenübermittlungskontrolle),

3.2.1.5. die Einrichtung eines Audit-Trails zur Dokumentation, ob und durch wen auf personenbezogene Daten zugegriffen wurde, sie geändert wurden oder aus den personenbezogenen Daten verarbeitenden Systemen entfernt wurden (Zugriffskontrolle),

3.2.1.6. sicherzustellen, dass die Verarbeitung personenbezogener Daten nur in Einklang mit den Weisungen des Kunden stattfindet (Weisungskontrolle),

3.2.1.7. sicherzustellen, soweit es dem Auftragsverarbeiter möglich ist, dass die personenbezogenen Daten gegen unbeabsichtigte Vernichtung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

3.2.1.8. sicherzustellen, soweit es dem Auftragsverarbeiter möglich ist, dass die für unterschiedliche Zwecke erfassten Daten getrennt verarbeitet werden können, und zwar auf der Grundlage der Weisungen des Kunden (Trennungskontrolle) sowie, sofern durchführbar, unter Einsatz branchenüblicher Verschlüsselung und/oder Pseudonymisierung.

3.2.2. Die Gesellschaft überwacht die Einhaltung der vorgenannten Maßnahmen in Abschnitt 3.2.1 in regelmäßigen Abständen. Während einer Abonnementlaufzeit verringert die Gesellschaft die Gesamtsicherheit der Software Services nicht in wesentlichem Umfang.

3.2.3. Zertifizierungen und Audits von Drittanbietern. Wie in der DPPSAD festgelegt, hat die Gesellschaft Zertifizierungen und Audits von Drittanbietern eingeholt. Auf schriftliche Aufforderung des Kunden und vorbehaltlich der Geheimhaltungspflichten des Vertrags stellt die Gesellschaft Kunden, bei denen es sich nicht um Wettbewerber der Gesellschaft (und nicht um unabhängige Auditoren des Kunden, die nicht Wettbewerber der Gesellschaft sind) handelt, in angemessenen Abständen eine Kopie der neusten Audits und Zertifizierungen von Drittanbietern aus der DPPSAD, in angemessenem Umfang zur Verfügung, wobei die berechtigten Interessen der Gesellschaft gewahrt bleiben.

4. Pflichten des Verantwortlichen

4.1. Der Kunde und die Gesellschaft sind getrennt voneinander verantwortlich für die Einhaltung der jeweils für sie geltenden gesetzlichen Vorschriften zum Datenschutz, einschließlich der Datenschutzgesetze und -verordnungen.

4.2. Der Kunde informiert die Gesellschaft unverzüglich und umfassend über Fehler und Unregelmäßigkeiten in Bezug auf die gesetzlichen Vorgaben für die Verarbeitung personenbezogener Daten, die im Zuge der Prüfung der Verarbeitungsergebnisse festgestellt wurden.

4.3. Der Kunde informiert die Gesellschaft unverzüglich und umfassend, falls:

4.3.1. er erkennt, dass bei der Nutzung der Software Services personenbezogene Daten verarbeitet werden, die Abschnitt 2.1 entgegenstehen, und er unternimmt umgehend die gegebenenfalls von der Gesellschaft geforderten Schritte, um seine Nutzung der Software Services in Einklang mit Abschnitt 2.1 zu bringen; und

4.3.2. besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO verarbeitet werden sollen oder aus anderen Gründen Auffälligkeiten bei der Beurteilung auftreten, insbesondere wenn eine erhöhte Wahrscheinlichkeit besteht, dass ernsthafte Risiken für die Rechte der betroffenen Person entstehen. Darüber hinaus beachtet der Kunde die Bestimmungen zu sensiblen Informationen im Vertrag und übermittelt der Gesellschaft eine Data Map vor Beginn der Verarbeitung besagter Daten.

4.4. Der Kunde hält sich in Bezug auf die Verarbeitung personenbezogener Daten im Rahmen der Datenschutzgesetze und -verordnungen an seine Pflichten als Verantwortlicher. Dies umfasst:

4.4.1. die allgemeinen Grundsätze des Datenschutzes (Artikel 1-5 DSGVO) und die Bearbeitung der Anträge betroffener Personen (Artikel 15-22 DSGVO),

4.4.2. die Erfüllung der Pflichten zu bestätigender Einwilligung (Artikel 4(11), 7 DSGVO), zu Information und Transparenz (Artikel 12-14 DSGVO) und zur Aufzeichnung (Artikel 30 DSGVO).

4.5. Bei Kündigung oder Beendigung des Vertrags legt der Kunde innerhalb einer von der Gesellschaft festgelegten Frist schriftlich fest, welche angemessenen Maßnahmen zu ergreifen sind, um Datenträger zurückzugeben oder gespeicherte Daten zu löschen.

4.6. Im gesetzlich erlaubten Umfang gehen in Verbindung mit der Rückgabe oder Löschung personenbezogener Daten nach Kündigung oder Beendigung des Vertrags entstehende zusätzliche Kosten zulasten des Kunden.

5. Rechte betroffener Personen

5.1. Im gesetzlich erlaubten Umfang benachrichtigt die Gesellschaft den Kunden unverzüglich, wenn die Gesellschaft einen

Antrag einer betroffenen Person bezüglich der Ausübung ihrer Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung („**Recht auf Vergessenwerden**"), Datenübertragbarkeit, Widerspruch gegen die Verarbeitung oder ihres Rechts, nicht einer auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, erhält („**Anfrage einer betroffenen Person**"). Je nach Art der Verarbeitung unterstützt die Gesellschaft den Kunden durch angemessene technische und organisatorische Maßnahmen soweit wie möglich bei der Erfüllung seiner Pflicht, den Anträgen betroffener Personen gemäß den Datenschutzgesetzen und -verordnungen nachzukommen. Falls der Kunde im Rahmen der Nutzung der Software Services nicht die Möglichkeit besitzt, den Anträgen betroffener Personen nachzukommen, wirkt die Gesellschaft auf Aufforderung des Kunden im Rahmen des Zumutbaren bei der Beantwortung der Anträge betroffener Personen mit, und zwar im gesetzlich erlaubten Rahmen und falls die Anträge der betroffenen Personen gemäß den Datenschutzgesetzen und -verordnungen zu beantworten sind. Im gesetzlich erlaubten Umfang trägt der Kunde die aus der Bereitstellung dieser zusätzlichen Hilfestellung entstehenden Kosten.

5.2. Damit die Gesellschaft im Rahmen des Zumutbaren bei der Beantwortung der Anträge betroffener Personen gemäß Abschnitt 5.1 dieses DPA mitwirken kann, kann die Gesellschaft vom Kunden eine Data Map der auf den Software Services aufbauenden Lösung des Kunden anfordern. Der Kunde hat sicherzustellen, dass er keine wiederholten oder anderweitig nicht qualifizierten Anträge betroffener Personen, wie in den Datenschutzgesetzen und -verordnungen definiert, an die Gesellschaft übersendet.

5.3. Ungeachtet der Abschnitte 5.1 und 5.2 bietet die Gesellschaft nur Hilfestellung bei Anträgen betroffener Personen, bei denen die fraglichen personenbezogenen Daten von der Gesellschaft verarbeitet werden, also nicht in Fällen, bei denen die personenbezogenen Daten außerhalb der Software Services, für die der Kunde verantwortlich ist, verarbeitet werden.

6. DPA-Audits

6.1. Der Kunde kann die technischen und organisatorischen Maßnahmen, welche die Gesellschaft in Zusammenhang mit der Verarbeitung im Rahmen der Software Services des Kunden ergriffen hat, vor Beginn der Verarbeitung und unter Beachtung der im Vertrag enthaltenen Geheimhaltungspflichten prüfen und muss die entsprechenden Ergebnisse dokumentieren. Dem Kunden steht es frei, einen unabhängigen Prüfer, der nicht im Wettbewerb mit der Gesellschaft steht, mit einer solchen Prüfung zu beauftragen. Die Leitlinien und Grundsätze einer solchen Prüfung sind im Vertrag zwischen den Parteien näher ausgeführt.

6.2. Zu diesem Zweck kann der Kunde

6.2.1. Informationen von der Gesellschaft (oder Unterauftragsverarbeitern der Gesellschaft) anfordern,

6.2.2. die Gesellschaft (oder Unterauftragsverarbeiter der Gesellschaft) auffordern, vorhandene Bestätigungen oder Zertifizierungen unabhängiger Experten an den Kunden zu übermitteln, oder

6.2.3. nach angemessener vorheriger Vereinbarung und während der regulären Geschäftszeiten Prüfungen des Geschäftsbetriebs der Gesellschaft auf alleinige Kosten des Kunden und ohne Störung der Geschäftsabläufe der Gesellschaft vor Ort vornehmen oder durch einen Dritten, der nicht im Wettbewerb mit der Gesellschaft steht, vornehmen lassen.

6.3. Auf schriftliche Aufforderung des Kunden stellt die Gesellschaft innerhalb einer angemessenen Frist alle für ein solches Audit verhältnismäßigen und erforderlichen Informationen bereit, sofern eine solche Offenlegung von Informationen nicht gegen Verträge und/oder Sicherheits- und andere Richtlinien und Verfahren der Gesellschaft verstößt. Werden bei einem Audit Verstöße oder mangelnde Konformität festgestellt, setzt der Kunde die Gesellschaft darüber unverzüglich in Kenntnis.

6.4. Im Sinne dieses Abschnitts 6 durchgeführte Audits:

6.4.1. werden nicht häufiger als einmal pro Kalenderjahr durchgeführt (sofern nicht anderweitig durch die staatliche Regulierungsstelle oder Aufsichtsbehörde vorgegeben),

6.4.2. werden mindestens 60 (sechzig) Tage im Voraus angekündigt, wobei der Kunde mindestens zwei Wochen vor dem geplanten Termin einen detaillierten Auditplan mit Umfang, Dauer und Startdatum des Audits übermittelt, den Optimizely dann prüft und genehmigt, und

6.4.3. können zu zusätzlichen Kosten führen, wenn die Kosten des Audits 2 % der jährlichen Gesamtzahlungsverpflichtung aus dem Master Services Agreement überschreiten.

7. Unterauftragsverarbeiter

7.1. **Ernennung von Unterauftragsverarbeitern.** Der Kunde erkennt an, dass (a) die verbundenen Unternehmen der Gesellschaft als Unterauftragsverarbeiter beauftragt werden können und (b) die Gesellschaft und die verbundenen Unternehmen der Gesellschaft jeweils Drittanbieter als Unterauftragsverarbeiter in Verbindung mit der Bereitstellung der Software Services beauftragen können. Die Gesellschaft oder ein verbundenes Unternehmen der Gesellschaft geht einen schriftlichen Vertrag mit jedem Unterauftragsverarbeiter ein, der Verpflichtungen zum Datenschutz enthält, die entsprechend der Art der von Unterauftragsverarbeiter bereitgestellten Software Services keinen geringeren Schutz in Bezug auf die Kundendaten bieten als diejenigen, die in diesem DPA und dem Vertrag festgeschrieben sind, und hält die Vorschriften bezüglich der Übermittlung personenbezogener Daten in Drittländer gemäß Artikel 44-50 DSGVO ein. Beinhaltet ein solches Vertragsverhältnis die Übermittlung personenbezogener Daten in Drittländer, stimmt der Kunde zu, dass die Gesellschaft

Standardvertragsklauseln eingeht, welche die Übermittlung von Auftragsverarbeiter zu Auftragsverarbeiter regeln. Der Verantwortliche autorisiert hiermit die Gesellschaft, derartige Standardvertragsklauseln mit den entsprechenden Unterauftragsverarbeitern in Drittländern zu unterzeichnen.

7.2. **Liste der aktuellen Unterauftragsverarbeiter und Benachrichtigung über neue Unterauftragsverarbeiter.** Die Gesellschaft stellt dem Kunden die aktuelle Liste der Unterauftragsverarbeiter für die in Annex III der Anlage zu Anhang 1 aufgeführten Dienstleistungen bereit. Diese Auflistung der Unterauftragsverarbeiter beinhaltet die Identität der Unterauftragsverarbeiter sowie das Land, in dem sie sich befinden („**Dokumentation zu Infrastruktur und Unterauftragsverarbeitern**"). Der Kunde kann die aktuelle Liste der Webpage mit den Trust Center Ressourcen der Gesellschaft entnehmen (auch abrufbar unter https://www.optimizely.com/trust-center/privacy/sub-processors/). Die Gesellschaft gibt eine Benachrichtigung über neue Unterauftragsverarbeiter heraus, bevor diese autorisiert werden, personenbezogene Daten in Verbindung mit der Bereitstellung der entsprechenden Services zu verarbeiten. Diese Benachrichtigung wird unter https://status.optimizely.com/ vorgenommen. Dieser Webpage ist auch die Funktion innerhalb des Abonnements zu entnehmen.

7.3. **Widerspruchsrecht bei neuen Unterauftragsverarbeitern.** Der Kunde kann der Einsetzung eines neuen Unterauftragsverarbeiters durch die Gesellschaft innerhalb von 30 (dreißig) Tagen schriftlich widersprechen, nachdem er von der Gesellschaft auf die im Vertrag festgelegte Weise benachrichtigt worden ist. Widerspricht der Kunde einem neuen Unterauftragsverarbeiter gemäß voranstehendem Satz, unternimmt die Gesellschaft im Rahmen des Zumutbaren Anstrengungen, um dem Kunden eine Änderung der Software Services zu ermöglichen oder eine wirtschaftlich machbare Änderung an der Konfiguration oder Nutzung der Software Services vorzuschlagen, um die Verarbeitung personenbezogener Daten durch den neuen Unterauftragsverarbeiter, gegen den Widerspruch eingelegt wurde, zu vermeiden, ohne den Kunden übermäßig zu belasten. Ist die Gesellschaft innerhalb eines angemessenen Zeitraums, der 30 (dreißig) Tage nicht überschreiten darf, nicht in der Lage, eine solche Änderung bereitzustellen, kann der Kunde den betreffenden Vertrag und/oder die betreffende Bestellung(en) für diejenigen Software Services, die von der Gesellschaft nicht ohne Inanspruchnahme des Unterauftragsverarbeiters, gegen den Widerspruch eingelegt wurde, bereitgestellt werden können, durch schriftliche Mitteilung an die Gesellschaft kündigen. Die Gesellschaft erstattet im Voraus bezahlte, nicht genutzte Gebühren für diese gekündigten Software Services ab dem Datum des Inkrafttretens der Kündigung zurück.

7.4. **Haftung.** Sofern nicht anderweitig im Vertrag festgelegt, ist die Gesellschaft für Handlungen und Unterlassungen ihrer Unterauftragsverarbeiter im selben Umfang haftbar, wie sie haftbar wäre, wenn sie die Leistungen des jeweiligen Unterauftragsverarbeiters gemäß den Bestimmungen dieses DPA direkt erbracht hätte.

8. Informationspflicht, Erfordernis der Schriftform, Rechtswahl, weitere Bestimmungen

8.1. Die Gesellschaft informiert den Kunden unverzüglich, wenn die personenbezogenen Daten des Kunden während ihrer Verarbeitung Gegenstand einer Durchsuchung und Beschlagnahme, eines Pfändungsbeschlusses, einer Beschlagnahme im Rahmen von Insolvenzverfahren oder ähnlicher Ereignisse bzw. Maßnahme vonseiten Dritter werden. Die Gesellschaft setzt alle an einem solchen Ereignis beteiligten Parteien unverzüglich darüber in Kenntnis, dass alle hiervon betroffenen personenbezogenen Daten alleiniges Eigentum des Kunden sind und dessen Verantwortung unterliegen, dass der Verantwortliche das alleinige Verfügungsrecht über die personenbezogenen Daten besitzt und dass der Verantwortliche im Sinne der Datenschutzgesetze und -verordnungen verantwortlich ist.

8.2. Die Gesellschaft ist berechtigt, nach vorheriger Mitteilung mit einer Frist von mindestens 90 (neunzig) Tagen Ergänzungen oder Änderungen an diesem DPA vorzunehmen, wenn diese Ergänzungen oder Änderungen nach ihrem Ermessen aufgrund von Änderungen der Datenschutzgesetze und -verordnungen erforderlich sind. Diese Ergänzungen oder Änderungen umfassen den Ersatz oder die Einführung weiterer SCCs zusätzlich zu denen in Anlage 1, und zwar in Form von Standarddatenschutzklauseln, die nach Artikel 46 DSGVO von Zeit zu Zeit verabschiedet werden, oder andere Änderungen der in Anhang 3 (Ergänzende Maßnahmen) beschriebenen Art. Unbeschadet der vorgenannten Bestimmungen dieses Abschnitts gelten die Bestimmungen in Abschnitt 10 'Ergänzungen; kein Verzicht' des EUSA.

8.3. Sind für die Bereitstellung der Software Services mehrere Transfermechanismen erforderlich, wird die Übermittlung personenbezogener Daten durch einen einzigen Transfermechanismus vorgenommen, wobei folgender Vorrang besteht: (1) die verbindlichen Unternehmensregeln für die Verarbeitung personenbezogener Daten (Company Processor BCR) und (2) die Standardvertragsklauseln.

8.4. Sind einzelne Bestimmungen dieses DPA unwirksam oder nicht durchsetzbar, bleiben die Wirksamkeit und Durchsetzbarkeit der übrigen Bestimmungen dieses DPA davon unberührt.

8.5. Die SCCs gelten für die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen des Vertrags. Durch Beifügung dieses DPAs zum Vertrag erklären sich die in Abschnitt 9 unten aufgeführten Parteien (Parteien dieses DPAs) mit den SCCs und allen zugehörigen Anlagen in ihrer jeweils gemäß Abschnitt 8.2 aktualisierten Form einverstanden.

8.6. Ungeachtet Abschnitt 8.7 gelten die SCCs nur für personenbezogene Daten, die aus dem Europäischen Wirtschaftsraum (EWR) nach außerhalb des EWRs entweder direkt übermittelt oder weitergeleitet werden in ein Land oder an einen Empfänger: das oder (i) kein von der Europäischen Kommission anerkanntes angemessenes Schutzniveau für

personenbezogene Daten (gemäß DSGVO) bietet, und (ii) nicht durch ein geeignetes und von den zuständigen Behörden oder Gerichten als angemessener Schutz personenbezogener Daten anerkanntes Rahmenwerk, wie verbindliche Unternehmensregeln für Auftragsverarbeiter, abgedeckt ist.

8.7. Handelt es sich bei den geltenden Datenschutzgesetzen und -verordnungen um die Rechtsvorschriften und Verordnungen des Vereinigten Königreichs, können die im Artikel 46 UK-DSGVO genehmigten SCCs auf personenbezogene Daten anwendbar sein, die entweder direkt übermittelt oder weitergeleitet werden in ein Land oder an einen Empfänger: das oder der (i) kein vom Data Protection Act 2018 anerkanntes angemessenes Schutzniveau für personenbezogene Daten (gemäß DSGVO) bietet, und (ii) nicht durch ein geeignetes und von den zuständigen Behörden oder Gerichten als angemessener Schutz personenbezogener Daten anerkanntes Rahmenwerk, wie verbindliche Unternehmensregeln für Auftragsverarbeiter, abgedeckt ist.

8.8. **Zusätzliche Bestimmungen für Europa**

8.8.1. DSGVO. Die Gesellschaft verarbeitet personenbezogene Daten in Einklang mit den Anforderungen der DSGVO, die auf die Bereitstellung der Software Services durch die Gesellschaft direkt anwendbar sind.

8.8.2. Datenschutz-Folgenabschätzung. Auf Bitte des Kunden wirkt die Gesellschaft bei der Erfüllung der Pflicht des Kunden gemäß DSGVO, eine Datenschutz-Folgenabschätzung bezüglich der Nutzung der Software Services durch den Kunden durchzuführen mit, falls der Kunde anderweitig keinen Zugang zu den relevanten Informationen hat und der Gesellschaft diese Informationen zur Verfügung stehen. Soweit gemäß DSGVO erforderlich, unterstützt die Gesellschaft den Kunden auf angemessene Weise bei der Zusammenarbeit oder der vorherigen Absprache mit der Aufsichtsbehörde bezüglich der Erfüllung seiner Pflichten in Bezug auf Abschnitt 8.8.2 dieses DPA.

8.8.3. Transfermechanismen der Datenübermittlungen. Vorbehaltlich der zusätzlichen Bestimmungen in Annex II des Anhangs 1 bietet die Gesellschaft unten aufgeführte Transfermechanismen, soweit sie den Datenschutzgesetzen und -verordnungen entsprechen, in der in Abschnitt 8.3 genannten Reihenfolge an, wenn personenbezogene Daten für die dieses DPA gilt, aus der Europäischen Union, dem Europäischen Wirtschaftsraum und/oder ihren Mitgliedstaaten, der Schweiz und dem Vereinigten Königreich in Länder übermittelt werden, die, im Sinne der Datenschutzgesetze und -verordnungen der vorgenannten Gebiete, kein angemessenes Datenschutzniveau bieten.

8.8.3.1. Die Company BCRs gelten für die im Vertrag und/oder in der/den Bestellung(en) aufgeführten Software Services und unterliegen diesem DPA;

8.8.3.2. Die SCCs in Anhang 1 zu diesem DPA gelten für die im Vertrag und/oder in der/den Bestellung(en) aufgeführten Software Services, die nur zu Supportzwecken für die Software Services der Gesellschaft erforderlich sind.

Die Transfermechanismen, auf die sich der vorliegende Abschnitt 8.8.3 bezieht, werden zur Verarbeitung personenbezogener Daten unter den in diesem DPA vorgesehen Einschränkungen und Kontrollen bereitgestellt und insbesondere unter der Voraussetzung, dass der Kunde:

8.8.3.3. keine personenbezogenen Daten unter Verstoß gegen die Verbote oder Einschränkungen der Software Services bezüglich der Verarbeitung personenbezogener Daten nach Abschnitt 2.1 verarbeitet und

8.8.3.4. die Gesellschaft über etwaige erforderliche Einschränkungen durch Geofencing nach Anhang 3 (Ergänzende Maßnahmen) in Kenntnis setzt, damit geeignete Maßnahmen zum Geofencing ergriffen werden können, und

entsprechend erkennt der Kunde an, dass er als Verantwortlicher allein zuständig für die Einhaltung der Anforderungen der Datenschutzgesetze und -verordnungen in Hinblick auf die Verarbeitung personenbezogener Daten gemäß diesem DPA ist. Dies beinhaltet Übermittlungen personenbezogener Daten unter Verstoß gegen Abschnitt 8.8.3.3 oder Verstöße durch mangelnde Umsetzung von Einschränkungen durch Geofencing aufgrund fehlender Benachrichtigung der Gesellschaft durch den Kunden über das entsprechende Erfordernis gemäß Abschnitt 8.8.3.4. Die Bestimmungen des Abschnitts 8.8.3 gelten gegebenenfalls unbeschadet des Abschnitts 2.4.3.

9. Parteien des DPAs

9.1. Im Abschnitt „GELTUNGSBEREICH DIESES DPAs“ ist angegeben, welche Gesellschaft Partei dieses DPAs ist. Darüber hinaus ist die in den Standardvertragsklauseln in Anhang 1 (oder anderen SCCs, die diese nach Anhang 3 (Ergänzende Maßnahmen) ersetzen) aufgeführte Gesellschaft Partei der SCCs. Jede andere, nicht aufgeführte Gesellschaft ist nicht Partei dieses DPAs oder der Standardvertragsklauseln. Handelt es sich bei der Gesellschaft um eine andere juristische Person als Optimizely Inc. oder Episerver, Inc., ist die Gesellschaft, welche die Pflichten des in den SCCs genannten Datenimporteurs im Auftrag von Optimizely Inc. oder Episerver, Inc., erfüllt, bezugnehmend auf den Abschnitt „Haftungsbeschränkungen” des Vertrags auf diesen DPA anwendbar.

9.2. Autorisierte verbundene Unternehmen. Die Parteien vereinbaren, dass der Kunde durch Unterzeichnung des Vertrags den DPA in eigenem Namen und auch im Namen seiner autorisierten verbundenen Unternehmen eingeht und dadurch einen gesonderten DPA zwischen der Gesellschaft und einem jeden dieser autorisierten verbundenen Unternehmen gemäß den Bestimmungen des Vertrags und dieses Abschnitts 9 und Abschnitts 10 begründet. Jedes autorisierte verbundene Unternehmen erkennt die aus diesem DPA und, in entsprechendem Umfang, dem Vertrag entstehenden Pflichten an. Zur

Klarstellung: autorisierte verbundene Unternehmen werden nicht Partei des Vertrags, sondern nur Partei des DPAs. Zugriff auf und Nutzung von Software Services und Kundendaten durch autorisierte verbundene Unternehmen müssen in Einklang mit den Bestimmungen des Vertrags stehen und jeder Verstoß gegen die Bestimmungen des Vertrags durch ein autorisiertes verbundenes Unternehmen ist als Verstoß des Kunden anzusehen.

9.2.1. Kommunikation. Der Kunde, der Partei des Vertrags ist, bleibt verantwortlich für die Koordination sämtlicher Kommunikation im Rahmen dieses DPAs und ist berechtigt, in Verbindung mit diesem DPA im Namen seiner autorisierten verbundenen Unternehmen Mitteilungen zu machen und entgegenzunehmen.

9.2.2. Rechte der autorisierten verbundenen Unternehmen. Ist ein autorisiertes verbundenes Unternehmen Partei des DPAs mit der Gesellschaft, ist es, soweit in den geltenden Datenschutzgesetzen und -verordnungen vorgesehen, berechtigt, die Rechte aus diesem DPA auszuüben und Rechtsbehelfe einzulegen, vorausgesetzt:

9.2.2.1. Sofern nicht die geltenden Datenschutzgesetze und -verordnungen vorschreiben, dass das autorisierte verbundene Unternehmen selbst direkt gegenüber der Gesellschaft die Rechte aus diesem DPA ausübt und Rechtsbehelfe einlegt, vereinbaren die Parteien, dass (i) nur der Kunde, der Partei des Vertrags ist, im Namen des autorisierten verbundenen Unternehmens diese Rechte ausübt oder Rechtsbehelfe einlegt und (ii) dass der Kunde, der Partei des Vertrags ist, diese Rechte aus dem Vertrag nicht für jedes autorisierte verbundene Unternehmen einzeln ausübt, sondern zusammengefasst für alle seine autorisierten verbundenen Unternehmen (wie beispielsweise unten in Abschnitt 9.2.4 ausgeführt).

9.2.2.2. Die Parteien vereinbaren, dass der Kunde, der Partei des Vertrags ist, bei der Durchführung von Audits zu den für den Schutz personenbezogener Daten relevanten Vorgehensweisen alle angemessenen Maßnahmen ergreift, um die Auswirkungen auf die Gesellschaft und ihre Unterauftragsverarbeiter gering zu halten, indem er mehrere Auditanfragen im Namen unterschiedlicher autorisierter verbundener Unternehmen zu einem einzigen Audit zusammenfasst.

10. Rechtswirksamkeit

Dieser DPA wird zwischen Kunde und Gesellschaft erst rechtlich bindend, wenn alle im Abschnitt „UNTERZEICHNUNG DIESES DPAs“ oben dargelegten formalen Schritte vollständig abgeschlossen sind.

Dieser Vertrag wurde von den bevollmächtigten Vertretern der Parteien ordnungsgemäß unterzeichnet:

Gesellschaft:	**Kunde:**
Unterschrift: _____	Unterschrift: _____
Name in Druckbuchstaben: _____	Name in Druckbuchstaben: _____
Funktion: _____	Funktion: _____
Ort und Datum: _____	Ort und Datum: _____

ANHANG 1

Standardvertragsklauseln (von Verantwortlichen an Auftragsverarbeiter)

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an Drittländer eingehalten werden.

(b) Die Parteien:

i. die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (nachfolgend jeweils „Datenexporteur“), und

ii. die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“),

haben sich mit diesen Standardvertragsklauseln (nachfolgend „Klauseln“) einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Annex I.B.

(d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

(a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 (1) und Artikel 46 (2)(c) der Verordnung (EU) 2016/679 sowie, in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter, Standardvertragsklauseln gemäß Artikel 28(7) der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

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

Klausel 3

Drittbegünstigte.

(a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:

i. Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7,
ii. Klausel 8.1(b), 8.9(a), (c), (d) und (e),
iii. Klausel 9(a), (c), (d) und (e),
iv. Klausel 12(a), (d) und (f),
v. Klausel 13,
vi. Klausel 15.1(c), (d) und (e),
vii. Klausel 16(e) und
viii. Klausel 18(a) und (b).

(b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe (a) unberührt.

Klausel 4

Auslegung

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

Klausel 5
Vorrang

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

Klausel 6

Beschreibung der Datenübermittlung(en)

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

Klausel 7

Kopplungsklausel

(a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und Annex I.A unterzeichnet.
(b) Nach Ausfüllen der Anlage und Unterzeichnung von Annex I.A wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in Annex I.A.
(c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

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

8.1 *Weisungen*

(a) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.
(b) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann.

8.2 *Zweckbindung*

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Annex I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3 *Transparenz*

Auf Antrag stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Annex II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen. Er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Antrag teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.4 *Richtigkeit*

Stellt der Datenimporteur fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Datenimporteur mit dem Datenexporteur zusammen, um die Daten zu löschen oder zu berichtigen.

8.5 *Dauer der Verarbeitung und Löschung oder Rückgabe der Daten*

Die Daten werden vom Datenimporteur nur für die in Annex I.B angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Datenimporteur nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Datenimporteurs gemäß Klausel 14(e), den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14 (a) in Einklang stehen.

8.6 *Sicherheit der Verarbeitung*

(a) Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu diesen Daten führt (nachfolgend „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs. Zur Erfüllung seiner Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Annex II aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

(b) Der Datenimporteur gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(c) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt

verfügbaren Informationen und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

(d) Unter Berücksichtigung der Art der Verarbeitung und der dem Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8.7 *Sensible Daten*

Soweit die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (nachfolgend „sensible Daten“), wendet der Datenimporteur die in Annex I.B beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8 *Weiterübermittlungen*

Der Datenimporteur gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die außerhalb der Europäischen Union (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) ansässig sind (nachfolgend „Weiterübermittlung“), sofern der Dritte sich mit der Bindung an diese Klauseln einverstanden erklärt oder falls:

i. die Weiterübermittlung an ein Land erfolgt, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,
ii. der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung gewährleistet,
iii. die Weiterübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder
iv. die Weiterübermittlung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9 *Dokumentation und Einhaltung der Klauseln*

(a) Der Datenimporteur bearbeitet Anfragen des Datenexporteurs, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.
(b) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.
(c) Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten Pflichten nachzuweisen, und auf Verlangen des Datenexporteurs ermöglicht er diesem, die unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung zu prüfen, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.
(d) Der Datenexporteur kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Datenimporteurs umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
(e) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben (b) und (c) genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 9

Einsatz von Unterauftragsverarbeitern

(a) Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens 30 (dreißig) Tage im Voraus in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Datenexporteur damit ausreichend Zeit ein, um vor der

Beauftragung des/der Unterauftragsverarbeiter/s Widerspruch gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Datenexporteur die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(b) Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich in Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.

(c) Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(d) Der Datenimporteur haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Datenimporteur geschlossenen Vertrag nachkommt. Der Datenimporteur benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.

(e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur – sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 10

Rechte betroffener Personen

(a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.

(b) Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Annex II unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

(c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben (a) und (b) befolgt der Datenimporteur die Weisungen des Datenexporteurs.

Klausel 11

Rechtsbehelf

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

(b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

(c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an:

i. eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,

ii. den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.

(d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80(1) der Verordnung (EU) 2016/679 vertreten werden kann.

(e) Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.

(f) Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12

Haftung

(a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

(b) Der Datenimporteur haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

(c) Ungeachtet von Buchstabe (b) haftet der Datenimporteur gegenüber der betroffenen Person und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

(d) Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Buchstabe (c) für durch den Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs für den Schaden entspricht.

(e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

(f) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe (e) haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

(g) Der Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

(a) Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist: Die Aufsichtsbehörde, die dafür verantwortlich ist sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert entsprechend der Angabe in Annex I.C als zuständige Aufsichtsbehörde.

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3(2) der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt und einen Vertreter gemäß Artikel 27(1) der Verordnung (EU) 2016/679 benannt hat: Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter nach Artikel 27(1) der Verordnung (EU) 2016/679 niedergelassen ist, fungiert entsprechend der Angabe in Anhang I.C als zuständige Aufsichtsbehörde.

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3(2) der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27(2) der Verordnung (EU) 2016/679 benennen zu müssen: Die Aufsichtsbehörde eines der Mitgliedstaaten, in denen die betroffenen Personen niedergelassen sind, deren personenbezogene Daten gemäß diesen Klauseln im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen übermittelt werden oder deren Verhalten beobachtet wird, fungiert entsprechend der Angabe in Anhang I.C als zuständige Aufsichtsbehörde.

(b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

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

Klausel 14

Lokale Rechtsvorschriften, die sich auf die Einhaltung der Klauseln auswirken

(a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23(1) der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

(b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe (a) insbesondere die folgenden Aspekte gebührend berücksichtigt haben:
   i. die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,
   ii. die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes, einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten, sowie die geltenden Beschränkungen und Garantien,
   iii. alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

(c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe (b) nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

(d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe (b) zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe (a) in Einklang stehen. Hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe (a) im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.

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

Klausel 15

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

15.1 *Benachrichtigung*

(a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen:
   i. wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt

werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

ii. (ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden (diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten).

(b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

(c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).

(d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben (a) bis (c) während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Die Buchstaben (a) bis (c) gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14(e) und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2 *Überprüfung der Rechtmäßigkeit und Datenminimierung*

(a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14(e).

(b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.

(c) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV – SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

(a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14(f).

(c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn:

i. der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe (b) ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

ii. der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

iii. der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

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

(d) Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe (c) übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung der Daten. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

(e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn (i) die Europäische Kommission einen Beschluss nach Artikel 45(3) der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder (ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist. Wenn dieses Recht keine Rechte als Drittbegünstigte zulässt, unterliegen diese Klauseln dem Recht eines anderen EU-Mitgliedstaats, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Schweden ist.

Klausel 18

Gerichtsstand und Zuständigkeit

(a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.
(b) Die Parteien vereinbaren, dass dies die Gerichte von Schweden sind.
(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.
(d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANLAGE zu den Standardvertragsklauseln

Die vorliegende Anlage ist Bestandteil der Klauseln. Die Mitgliedstaaten können diese Anlage entsprechend ihrer nationalen Verfahrensweisen mit zusätzlichen Informationen vervollständigen oder präzisieren.

ANNEX I

A. LISTE DER PARTEIEN

Datenexporteur. Der Datenexporteur ist der im Vertrag (z. B. im Master Services Agreement „MSA" oder Master Managed Services Agreement „MMSA") und/oder in der/den Bestellung(en) angegebene **Kunde**.

Datenimporteur. Der Datenimporteur ist im Vertrag (z. B. im Master Services Agreement „MSA" oder Master Managed Services Agreement „MMSA") und/oder in der/den Bestellung(en) angegeben.

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen

Content/Commerce Clouds, Personalization: Die übermittelten personenbezogenen Daten betreffen die Endbenutzer des Kunden, einschließlich der Mitarbeiter, der Auftragnehmer und des Personals von Kunden, Lieferanten, Geschäftspartnern und Unterauftragnehmern. Zu den betroffenen Personen zählen auch Einzelpersonen, die versuchen, mit den Endbenutzern des Kunden zu kommunizieren oder personenbezogene Daten an sie zu übermitteln.

Experimentation/Full Stack: Die übermittelten personenbezogenen Daten betreffen die Endbenutzer sowie Besucher der Webseite und Apps des Kunden.

Optimizely Data Platform: Die übermittelten personenbezogenen Daten betreffen die Endbenutzer des Kunden, einschließlich der Mitarbeiter, der Auftragnehmer und des Personals von Kunden, Lieferanten, Geschäftspartnern und Unterauftragnehmern. Zu den betroffenen Personen zählen auch Einzelpersonen, die versuchen, mit den Endbenutzern des Kunden zu kommunizieren oder personenbezogene Daten an sie zu übermitteln.

Kategorien der übermittelten personenbezogenen Daten

Content/Commerce Clouds, Personalization: Bei den übermittelten Daten handelt es sich um personenbezogene Daten, Einrichtungsdaten (einschließlich Informationen zur Webseitennutzung), E-Mail-Daten, Systemnutzungsdaten, Anwendungsintegrationsdaten und andere Daten in elektronischer Form, die Endbenutzer über den/die Software Service(s) und/oder Managed Service(s) übermitteln, speichern, senden oder erhalten.

Experimentation/Full Stack: Bei den übermittelten personenbezogenen Daten handelt es sich um:

- Webseiten- und App-Besucher: IP-Adressen, Random Unique Identifiers, wie Cookie-IDs oder ähnliche Kennungen, sowie Experiment- und Ereignisdaten, die zu diesen Kennungen gehören (wie Gerätetyp, Varianten- und Experiment-IDs, Browser- und Betriebssystemversion sowie die Elemente der getesteten Seite) und auf der Nutzung und Konfiguration der Optimizely Services basieren. Der Kunde kann die Funktionen des Optimizely Services, wie die Anonymisierung der IP-Adresse, nutzen, um die Erfassung dieser Daten zu minimieren, und muss die Verbote des Hauptvertrags die Beschränkungen der Erfassung und Nutzung personenbezogener Daten betreffend einhalten.
- Endbenutzer des Kunden: Namen, E-Mail-Adressen, Passwörter, Kontaktdetails und ähnliche personenbezogene Daten, die von den Endbenutzern des Kunden bei der Erstellung eines Optimizely-Kontos bereitgestellt werden.

Optimizely Data Platform: Bei den übermittelten personenbezogenen und nicht personenbezogenen Daten handelt es sich um:

- Webseiten- und App-Besucher: IP-Adressen, Random Unique Identifiers, wie Cookie-IDs oder ähnliche Kennungen, und Ereignisdaten, die zu diesen Kennungen gehören (wie Gerätetyp, Browser- und Betriebssystemversion sowie die Elemente der getesteten Seite) und auf der Nutzung und Konfiguration der Optimizely Services basieren. Der Kunde kann die Funktionen des Optimizely Services nutzen, um die Erfassung dieser Daten zu minimieren, und muss die Verbote des Hauptvertrags die Beschränkungen der Erfassung und Nutzung personenbezogener Daten betreffend einhalten.
- Endbenutzer des Kunden: Namen, E-Mail-Adressen, Passwörter, Kontaktdetails und ähnliche personenbezogene Daten, die von den Endbenutzern des Kunden bei der Erstellung eines Optimizely-Kontos bereitgestellt werden.

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

Alle Software Services: Die Parteien gehen nicht von einer Übermittlung besonderer Kategorien von Daten aus.

Häufigkeit der Übermittlung

Alle Software Services: Die Daten werden kontinuierlich übermittelt.

Art der Verarbeitung

Alle Software Services: Der Kunde bestimmt die Art der Daten, die er an die Gesellschaft zur Verarbeitung in seinem Auftrag und im Zuge der Nutzung der Services der Gesellschaft übermittelt. Die Gesellschaft steht in keiner direkten Beziehung mit den Personen, deren Informationen sie von ihren Kunden oder deren Geschäftspartnern erhält. Die Gesellschaft hat keine Kontrolle über diese Daten, wählt oder bestimmt die spezifischen Arten der Daten, die sie verarbeitet, nicht und legt den Zweck, für den sie verarbeitet werden, nicht fest.

Davon abgesehen kann die Gesellschaft personenbezogene Daten in folgenden Fällen erfassen: bei der Erbringung von Expertenservices, die von dem Kunden angefragt werden, im Rahmen des Kundensupports, bei der allgemeinen Pflege der Kundenbeziehungen, wozu unter anderem Marketingaktivitäten, die Ausführung von Produktbestellungen, die Verbesserung des Produktangebots, Kundenumfragen, Fragebögen, die Beantwortung von Kommentaren oder ähnlichem zählen; darüber hinaus beim Herunterladen von Software und/oder bei Zugang zu bzw. Aktivierung von Produkten oder Dienstleistungen, für interne Geschäftszwecke, wie Finanzvorgänge oder die Beantwortung von Informationsersuchen, und für die Einhaltung geltender Rechtsvorschriften.

Experimentation/Full Stack: Zusätzlich zu oben Genanntem wird die Gesellschaft die Funktionen Flagging, Personalisierung, Analytics und/oder Software Services, die vom Kunden bestellt wurden, gemäß den Weisungen anbieten. Die Gesellschaft wird den Endbenutzern des Kunden zudem Berichte, Mitteilungen und andere von der Gesellschaft angebotene Funktionen bereitstellen.

Zwecke der Datenübermittlung und Weiterverarbeitung

Alle Software Services: Personenbezogene Daten können für folgende Zwecke verarbeitet werden: (a) zur Bereitstellung der Software Service (was die Erkennung, Vermeidung und Lösung von Problemen bezüglich Sicherheit und Technik beinhalten kann); (b) zur Beantwortung von Anfragen an den Kundensupport und (c) zur anderweitigen Erfüllung der Pflichten aus dem End-User Services Agreement und Service Level Agreement der Gesellschaft oder aus den Geschäftsbedingungen für Managed Services und dem Service Level Agreement (für Kunden der Managed Services) der Gesellschaft. Der Kunde weist die Gesellschaft an, personenbezogene Daten in Ländern zu verarbeiten, in denen die Gesellschaft oder ihre Unterauftragsverarbeiter Einrichtungen besitzen, die zur Erbringung des/der Software Service(s) notwendig sind.

Dauer der Datenverarbeitung

Alle Software Services: Der Zeitraum, für den die Daten verarbeitet werden, ist im Company End-User Services Agreement oder in den Geschäftsbedingungen für Managed Services (für Kunden der Managed Services) der Gesellschaft festgelegt. Für die Laufzeit des End-User Services Agreements oder der Geschäftsbedingungen für Managed Services (für Kunden der Managed Services) sowie für einen angemessenen Zeitraum nach Beendigung des Vertrags, ermöglicht der Datenimporteur dem Kunden den Zugang zu den personenbezogenen des Kunden, die gemäß dem Vertrag verarbeitet werden, und stellt sicher, dass diese exportiert werden können.

Datenlöschung

Alle Software Services: Während der Laufzeit des Vertrags ermöglicht die Gesellschaft dem Kunden, Daten gemäß dem Vertrag zu löschen.

Zugang zu Daten

Alle Software Services: Während der Laufzeit des Vertrags ermöglicht die Gesellschaft dem Kunden, personenbezogene Daten des/der Software Service(s) und/oder Managed Service(s) in Einklang mit dem Vertrag zu berichtigen, zu sperren, zu exportieren und zu löschen.

Unterauftragsverarbeiter

Alle Software Services: Die Gesellschaft kann Unterauftragsverarbeiter beauftragen, Teile des/der Software Services und/oder Managed Services bereitzustellen. Die Gesellschaft stellt sicher, dass sich der Zugang zu und die Nutzung von personenbezogenen Daten des Kunden durch Unterauftragsverarbeiter auf die Bereitstellung von Produkten und Dienstleistungen der Gesellschaft beschränken und keinem anderen Zweck dienen. Für nähere Angaben siehe Annex III.

C. BESCHREIBUNG DER DATENÜBERMITTLUNG

Schwedische Behörde für Datenschutz (Datainspektionen)

ANNEX II. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Nähere Angaben zu den technischen und organisatorischen Maßnahmen für die Software Services, welche die Gesellschaft dem Kunden bereitstellt, sind zu finden unter https://www.optimizely.com/trust-center/privacy/toms/.

ANNEX III. LISTE DER UNTERAUFTRAGSVERARBEITER

Der Kunde ermächtigt die Gesellschaft, die unter https://www.optimizely.com/trust-center/privacy/sub-processors/ aufgeführten Unterauftragsverarbeiter, die für die Bereitstellung der Software Services an den Kunden durch die Gesellschaft eingesetzt werden, zu beauftragen.

HQ (Americas / APJ)
119 5th Ave, 7th Floor | New York, NY 10003 | USA
+1 630 974 3000

HQ (EMEA)
Torsgatan 11 | Box 7007 | 103 86 Stockholm | Sweden
Reg. #: 556208-3435
+46 8 55 58 27 00

ANHANG 2 – Nähere Angaben zu Verarbeitung, Kategorien von Daten und betroffenen Personen

Art und Zweck der Verarbeitung

Die Gesellschaft verarbeitet personenbezogene Daten in dem Umfang, wie es zur Bereitstellung der Software Services gemäß Vertrag, den näheren Angaben in der Dokumentation und den Weisungen des Kunden während der Nutzung der Software Services erforderlich ist.

Dauer der Verarbeitung

Vorbehaltlich Abschnitt 8 der DPA, verarbeitet die Gesellschaft personenbezogene Daten für die Laufzeit des Vertrags, sofern nicht anderweitig schriftlich vereinbart.

Kategorien betroffener Personen

Der Kunden kann personenbezogene Daten an die Software Services senden, und zwar in einem Umfang, der im alleinigen Ermessen des Kunden festgelegt und gesteuert wird und unter anderem personenbezogene Daten folgende Kategorien betroffener Personen enthalten kann:

- Potenzielle Kunden, Kunden, Geschäftspartner und Anbieter des Kunden (als natürliche Personen)
- Mitarbeiter oder Kontaktpersonen von potenziellen Kunden, Kunden, Geschäftspartnern und Anbietern des Kunden
- Mitarbeiter, Handlungsbevollmächtigte, Berater, Freiberufler des Kunden (als natürliche Personen)
- Benutzer des Kunden, die vom Kunden zur Nutzung der Software Services autorisiert wurden

Arten personenbezogener Daten

Der Kunden kann personenbezogene Daten an die Software Services senden, und zwar in einem Umfang, der im alleinigen Ermessen des Kunden festgelegt und gesteuert wird und unter anderem folgende Kategorien personenbezogener Daten enthalten kann:

- Vor- und Zuname
- Anrede
- Position
- Arbeitgeber
- Kontaktinformationen (Unternehmen, E-Mail, Telefon, Geschäftsanschrift)
- Identifikationsnummern
- Daten zum beruflichen Werdegang
- Daten zum Privatleben
- Verbindungsdaten
- Standortdaten
- Cookie-IDs
- IP-Adresse
- Marketing Automation System IDs

Data Map

Wie in Abschnitt 5.2 dieser DPA beschrieben, hat der Kunde der Gesellschaft eine Data Map der Kategorien personenbezogener Daten und betroffener Personen zu übermitteln. Die Data Map und ihre folgenden Aktualisierungen sind als Teil des Anhangs 2 beizufügen.

Unterauftragsverarbeiter

Die Gesellschaft kann Unterauftragsverarbeiter beauftragen, Teile der Software Services bereitzustellen. Die Gesellschaft stellt sicher, dass sich der Zugang zu und die Nutzung von personenbezogenen Daten des Kunden durch Unterauftragsverarbeiter auf die Bereitstellung von Produkten und Dienstleistungen der Gesellschaft beschränken und keinem anderen Zweck dienen. Siehe Annex III der Anlage zu den Standardvertragsklauseln in Anhang 1 sowie https://www.optimizely.com/trust-center/privacy/sub-processors/.

ANHANG 3 – Ergänzende Maßnahmen

Im Lichte des Urteils „Schrems II“ des EuGH (Rechtssache C-311/18), nach dem die Verwendung von Standardvertragsklauseln ergänzende Maßnahmen erfordern kann, um einen angemessenen Datenschutz gemäß DSGVO bei der Übermittlung personenbezogener Daten in Drittländer zu gewährleisten, haben sich die Parteien auf Folgendes geeinigt.

1. Allgemeine Bestimmungen

Die Bestimmungen des vorliegenden Anhangs 3 ergänzen die für diesen DPA geltenden Standardvertragsklauseln. Darüber hinaus gelten die Bestimmungen des Abschnitts 2 für den DPA allgemein.

2. Geofencing

2.1. Die Gesellschaft hat Verfahrensweisen und Kontrollen eingerichtet, die es ermöglichen, die Übermittlung personenbezogener Daten in ein/e oder mehrere Hoheitsgebiete oder Regionen, in dem/der/denen sie, ihre verbundenen Unternehmen und Unterauftragsverarbeiter tätig sind, zu beschränken, wenn für die betreffende Datenbank, in der die personenbezogenen Daten gespeichert sind, Folgendes gilt:

2.1.1. Der Kunde hält ein Geofencing für notwendig und hat die Gesellschaft davon (über das unter www.optimizely.com/trust-center/privacy/geofencing festgelegte Verfahren) benachrichtigt oder

2.1.2. die Gesellschaft, ihre verbundenen Unternehmen und Unterauftragsverarbeiter haben erkannt, dass die Datenbank personenbezogene Daten enthält, die ein Geofencing erfordern,

um die von den Datenschutzgesetzen und -verordnungen geforderten Verbote und/oder Beschränkungen bei der Übermittlung einzuhalten. Die entsprechenden Verfahrensweisen und Kontrollen, über die die Beschränkungen des Geofencings umgesetzt werden, verhindern:

2.1.3. dass die Gesellschaft und ihre verbundenen Unternehmen diese personenbezogenen Daten in den betreffenden Hoheitsgebieten oder Regionen hosten und/oder

2.1.4. dass die Unterauftragsverarbeiter in den betreffenden Hoheitsgebieten oder Regionen im Zuge der Bereitstellung der Software Services auf die personenbezogenen Daten zugreifen oder diese anderweitig verarbeiten.

Nähere Angaben zu den Möglichkeiten des Geofencings sind unter www.optimizely.com/trust-center/privacy/geofencing zu finden. Sie können bisweilen von der Gesellschaft aktualisiert werden.

2.2. In Bezug auf das Geofencing erklärt sich der Kunde damit einverstanden:

2.2.1. als Verantwortlicher allein dafür zuständig zu sein, alle Datenbanken, die personenbezogene Daten enthalten, die im Rahmen dieses DPA verarbeitet werden und Beschränkungen durch Geofencing erfordern, zu identifizieren und diese der Gesellschaft mitzuteilen. Die Gesellschaft ist berechtigt, die ihr mitgeteilten Beschränkungen durch Geofencing umzusetzen und einzuhalten. Bis zu einer solchen Mitteilung ist die Gesellschaft berechtigt, diese personenbezogenen Daten gemäß den Bestimmungen des Abschnitts 3.1.5 dieses DPA ohne Beschränkung durch Geofencing zu verarbeiten.

2.2.2. dass die Gesellschaft, ein verbundenes Unternehmen oder ein Unterauftragsverarbeiter, die/der im Zuge der Bereitstellung von Support-Leistungen einen Datensatz identifiziert, der personenbezogene Daten enthält, die ihrer/seiner Ansicht nach eine Beschränkung durch Geofencing erfordern, berechtigt ist, eine solche Beschränkung anzuwenden und die erforderlichen Schritte zu ihrer Umsetzung zu unternehmen. Wird gemäß dem vorliegenden Abschnitt 2.2.2 des Anhangs 3 eine Beschränkung durch Geofencing angewendet, setzt die Gesellschaft den Kunden darüber umgehend in Kenntnis und darf diese weiter anwenden, und

2.2.3. Wird eine Beschränkung durch Geofencing angewendet, erteilt der Kunde der Gesellschaft, deren verbundenen Unternehmen oder Unterauftragsverarbeitern keine Weisung, die dazu im Widerspruch steht, und die Gesellschaft verstößt nicht gegen den Vertrag (einschließlich dieses DPAs), wenn er eine solche Weisung nicht befolgt.

3. Sonstige ergänzende Maßnahmen

3.1. Die Parteien vereinbaren, in gutem Glauben eng zusammenzuarbeiten und gegebenenfalls weitere ergänzende Maßnahmen (z. B. die Verbesserung vorhandener (oder die Umsetzung zusätzlicher) technischer und organisatorischer Sicherheitsmaßnahmen) in Verbindung mit der Verarbeitung personenbezogener Daten durch die Gesellschaft gemäß diesem DPA, die in Zusammenhang mit den im Urteil „Schrems II“ vorgesehenen Kriterien geeignet sein könnten, zu ergreifen.

3.2. Die Parteien vereinbaren, dass sich das Recht des Kunden, die Pflichten der Gesellschaft gemäß diesem DPA (einschließlich der Standardvertragsklauseln) zu überwachen und zu prüfen, auch auf die Pflichten der Gesellschaft gemäß dem vorliegenden Anhang 3 erstreckt.

HQ (Americas / APJ)
119 5th Ave, 7th Floor | New York, NY 10003 | USA
+1 630 974 3000

HQ (EMEA)
Torsgatan 11 | Box 7007 | 103 86 Stockholm | Sweden
Reg. #: 556208-3435
+46 8 55 58 27 00

3.3. Falls und soweit für den normalen Ablauf der Bereitstellung der durch den DAP abgedeckten Software Services erforderlich, willigt der Kunde ein, dass die Gesellschaft auf personenbezogene Daten, die in Plain Text übermittelt werden, zugreift.

4. Zusätzliche Pflichten des Kunden

4.1. Zusätzlich zu den Anforderungen des Abschnitts 8.3 der Standardvertragsklauseln in Anhang 1, ist der Kunde bei der Übermittlung aller Arten personenbezogener Daten verpflichtet, die betroffenen Personen gemäß Artikel 13 und 14 DSGVO darüber zu informieren, dass ihre Daten in ein Drittland übermittelt werden, das keinen angemessenen Schutz im Sinne der DSGVO bietet.

4.2. Erhält der Kunde von der Gesellschaft eine Benachrichtigung gemäß Klausel 15 der Standardvertragsklauseln in Anhang 1, setzt er die entsprechende(n) betroffenen Person(en) über dieses rechtlich bindende Ersuchen um Offenlegung personenbezogener Daten durch eine Justizbehörde, staatlicher Sicherheitsbehörde oder anderer Behörde („**Behörde**“) umgehend in Kenntnis, sofern es für den Kunden nicht unmöglich oder gesetzlich verboten ist, die betroffene Person zu informieren.

5. Zusätzliche Pflichten der Gesellschaft

5.1. Auf Aufforderung und soweit gesetzlich gestattet, informiert die Gesellschaft den Kunden in groben Zügen über die Zugangsersuchen von Behörden, welche die im Rahmen dieses DPAs verarbeiteten personenbezogenen Daten betreffen. Diese Informationen umfassen mindestens die Anzahl der Ersuchen, die Art der angefragten Daten, die rechtliche Grundlage für derartige Ersuchen und die ersuchenden Behörden, sofern die Bereitstellung dieser Informationen sich nicht als unmöglich erweist oder anderweitig von Rechts wegen verboten ist. In letzterem Fall ist Abschnitt 4.1 dieses Anhangs 3 anzuwenden.

5.2. Auf Aufforderung stellt die Gesellschaft dem Kunden alle Informationen, Dokumentationen und angemessen Hilfestellung wie erforderlich bereit, damit der Kunde den Anforderungen für die Übermittlung personenbezogener Daten an die Gesellschaft gemäß Artikel 44ff. DSGVO (einschließlich offizieller Richtlinien von EU-Aufsichtsbehörden und relevanter Gerichtsurteile) genügen kann.

5.3. In Einklang mit Klausel 14 der Standardvertragsklauseln in Anhang 1 bestätigt die Gesellschaft, dass sie keinen Grund zu der Annahme hat, dass zum Zeitpunkt des Beitritts zu den Klauseln lokale Rechtsvorschriften und Gepflogenheiten bestehen, die sich in wesentlichem Umfang auf die in Anhang 1 (wie zutreffend) und Anlage 3 enthaltenen Bestimmungen nachteilig auswirken.

5.4. Die Gesellschaft verpflichtet sich, die geltenden Rechtsvorschriften und Verordnungen zum Zugang zu personenbezogenen Daten durch Behörden sowie die nach geltenden Rechtsvorschriften und Verordnungen ergriffenen Garantien und rechtlichen Mittel zum Schutz betroffener Personen zu prüfen und auszuwerten und den Kunden im Falle von Änderungen der geltenden Rechtsvorschriften und Verordnungen, die sich auf die Rechte und Interessen betroffener Personen in wesentlichem Maß nachteilig auswirken, so schnell wie möglich zu informieren.

5.5. Die Gesellschaft versichert, dass sie, was die bereitgestellten Software Services betrifft, (i) nicht absichtlich Backdoors erzeugt oder andere Programmierungen vorgenommen hat oder vornehmen wird, die Behörden den Zugang zum System und/oder zu personenbezogenen Daten erlauben, (ii) ihre Geschäftsabläufe nicht absichtlich auf eine Weise entwickelt oder geändert hat bzw. entwickeln oder ändern wird, die den Zugang von Behörden auf personenbezogene Daten oder Systeme erleichtert, und (iii) keine Kenntnis von Anforderungen der nationalen Rechtvorschriften oder Vorschriften der Regierung hat, welche die Gesellschaft zwingen, Backdoors zu erzeugen oder vorzuhalten bzw. den Zugang zu personenbezogenen Daten oder Systemen durch Behörden zu erleichtern oder im Besitz des Verschlüsselungscodes zu sein bzw. diesen in diesem Zusammenhang an die Behörden zu übergeben. Unbeschadet anderer Rechte des Kunden, hat der Kunde das Recht, diesen DPA und den Vertrag fristlos zu kündigen, falls die Gesellschaft gegen den vorliegenden Abschnitt 5.5 verstößt.

6. Drittbegünstigtenklausel

6.1. Betroffene Personen können ihre Rechte gegenüber der Gesellschaft gemäß dem vorliegenden Abschnitt 6 des Anhangs 3 sowie den Abschnitten 1, 3.5 und 3.6 unter den in Klausel 3(a) der Standardvertragsklauseln in Anhang 1 festgelegten Bedingungen als Drittbegünstigte geltend machen.