Datenverarbeitungsvertrag und Standardvertragsklauseln nach DSGVO

Dieser Datenverarbeitungsvertrag nach DSGVO („**Vertrag**“) wird zwischen der nachfolgend angegebenen juristischen Person als Verantwortlichem (der „**Verantwortliche**“) und Proofpoint, Inc., 925 W. Maude Avenue, Sunnyvale, CA 94085 („**Auftragsverarbeiter**” oder „**Proofpoint**“) geschlossen und einer der folgenden Vereinbarungen als Anhang beigefügt: (1) dem Abonnement-Rahmenvertrag (Master Subscription Agreement) oder den Allgemeinen Geschäftsbedingungen von Proofpoint und der/den jeweiligen produktspezifischen Anlage(n), (2) einem Endnutzer-Lizenzvertrag (in Form einer Online-Kundenvereinbarung, eines EULA oder einer in elektronischer Form verfügbaren Clickwrap-Lizenz oder Clickthrough-Vereinbarung), den der Verantwortliche bei seiner erstmaligen Registrierung und mit erstmaligem Zugriff auf die Produkte oder Dienste von Proofpoint akzeptiert, oder (3) einer anderen schriftlichen, unterzeichneten Lizenzvereinbarung zwischen den Parteien, in deren Rahmen der Auftragsverarbeiter dem Verantwortlichen Produkte oder Dienstleistungen bereitstellt (der „**Servicevertrag**“). Dieser Vertrag tritt mit dem Datum der Unterzeichnung durch den Verantwortlichen in Kraft, jedoch nur, wenn der unterzeichnete Vertrag gemäß den nachstehenden Anweisungen bei Proofpoint eingeht.

In diesem Vertrag sind die Bedingungen festgelegt, unter denen der Auftragsverarbeiter personenbezogene Daten vom Verantwortlichen erhält und verarbeiten darf. Der Vertrag berücksichtigt die Art der Verarbeitung gemäß dem Servicevertrag und beschreibt die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten.

Darüber hinaus sind in diesem Vertrag die Standardvertragsklauseln enthalten, die der Anlage des Beschlusses der Kommission 2021/914 beiliegen (die „**SVK**“). Zusätzlich zu den in diesem Vertrag festgelegten Pflichten erfüllt Proofpoint die Pflichten eines Datenimporteurs gemäß den SVK. Alle Bezugnahmen auf den **Datenimporteur** gelten als Bezugnahmen auf **Proofpoint, Inc. oder den Auftragsverarbeiter**, und alle Bezugnahmen auf den **Datenexporteur** oder den Datenverantwortlichen gelten als Bezugnahmen auf den **Verantwortlichen** und seine verbundenen Unternehmen in der Europäischen Union. Der Verantwortliche sichert hiermit ausdrücklich zu, dass er zum Abschluss und der Erfüllung dieses Vertrages in eigenem Namen und für seine verbundenen Unternehmen berechtigt und befugt ist.

Die Parteien dieses Vertrags erkennen hiermit die Bedingungen und Bestimmungen in der beigefügten Anlage 1 (Datenschutzbestimmungen) und dessen Anhängen und Anlage 2 (Standardvertragsklauseln) als verbindlich an. Dieser Vertrag wurde vom Auftragsverarbeiter Proofpoint, Inc. vor unterzeichnet. Damit dieser Vertrag wirksam wird, muss der Verantwortliche zunächst:

1. nachstehend den vollständigen Namen der juristischen Person des Verantwortlichen, die Anschrift und Angaben zum Unterzeichner eintragen und unterzeichnen und
2. den ausgefüllten und unterzeichneten Vertrag per E-Mail an privacy@proofpoint.com an Proofpoint senden.

Streichungen oder sonstige Änderungen an diesem Vertrag, die der Verantwortliche ohne vorherige Absprache mit Proofpoint vornimmt, werden hiermit zurückgewiesen und sind unwirksam. Der Unterzeichner des Verantwortlichen sichert ausdrücklich zu, dass er berechtigt ist, den Verantwortlichen an diesen Vertrag zu binden. Dieser Vertrag endet automatisch mit der Beendigung des Servicevertrags oder im Falle einer Kündigung dieses Vertrages gemäß den Bestimmungen dieses Vertrags, je nachdem, was zuerst eintritt.

Angenommen und genehmigt vom Verantwortlichen:	Angenommen und genehmigt von **Proofpoint, Inc.:** (**Auftragsverarbeiter**)
Unterschrift: _____	Unterschrift: DocuSigned by: Paul Auvil 2955B8CEBD2B45C...
Name: _____	Name: Paul Auvil, CFO
Datum: _____	
Firma: _____	
Anschrift: _____	
_____	

ANLAGE 1

BESTIMMUNGEN FÜR DIE DATENVERARBEITUNG

1. Begriffsbestimmungen.

a. Alle in diesem Vertrag nicht definierten Begriffe haben vorrangig die in der EU-Datenschutz-Grundverordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (**DSGVO**) beschriebene Bedeutung; nachfolgend haben sie die Bedeutung, die ihnen gemäß Servicevertrag zugewiesen ist.

b. **Daten des Verantwortlichen** sind die personenbezogenen Daten des Verantwortlichen, wobei die Definition für personenbezogene Daten dieselbe ist wie in der Datenschutz-Grundverordnung.

c. **Datenschutzgesetze** bezeichnet alle anwendbaren Gesetze und anderen Rechtsvorschriften über die Verarbeitung personenbezogener Daten, soweit sie mit der Bereitstellung der Produkte und der Erbringung von Serviceleistungen durch Proofpoint gemäß Servicevertrag im Zusammenhang stehen.

d. **Betroffene Person** bezeichnet die identifizierte oder identifizierbare Person, auf die sich die personenbezogenen Daten beziehen.

e. **Verarbeitung** (und damit verwandte Begriffe) hat die diesem Begriff in Artikel 4 Absatz 2 der DSGVO zugewiesene Bedeutung.

f. **Unterauftragsverarbeiter** bezeichnet einen Verarbeiter, der von Proofpoint mit der Verarbeitung personenbezogener Daten beauftragt wird.

g. **Aufsichtsbehörde** bezeichnet eine von einem EU-Mitgliedstaat gemäß DSGVO errichtete staatliche Stelle.

2. Verarbeitung personenbezogener Daten.

a. Die Parteien beabsichtigen, dass der Verantwortliche und seine in der Europäischen Union ansässigen verbundenen Unternehmen (oder deren verbundene Unternehmen oder Kunden) in Bezug auf die in Anhang 1 beschriebenen Tätigkeiten als Datenverantwortliche/Datenexporteur gelten und der Auftragsverarbeiter als Datenverarbeiter/Datenimporteur, soweit er personenbezogene Daten verarbeitet. Der Verantwortliche stimmt ausdrücklich zu, dass seine Anweisungen an den Auftragsverarbeiter hinsichtlich der Verarbeitung personenbezogener Daten im Einklang mit den maßgeblichen Bestimmungen der geltenden Datenschutzgesetze stehen.

b. Gegenstand und Dauer der Verarbeitung personenbezogener Daten sind im Servicevertrag festgelegt, der die Bereitstellung der Serviceleistungen an den Verantwortlichen regelt. Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind Anhang 1 dieses Vertrags zu entnehmen.

c. Der Verantwortliche ist für die Richtigkeit, Zustand und Rechtmäßigkeit der personenbezogenen Daten und die Art und Weise, auf die er die personenbezogenen Daten erhoben hat, verantwortlich.

d. Der Servicevertrag und dieser Vertrag bilden hiermit die Anweisungen des Verantwortlichen an den Auftragsverarbeiter in Bezug auf: (1) die Verarbeitung personenbezogener Daten und (2) die Übermittlung solcher personenbezogenen Daten in ein beliebiges Land oder Hoheitsgebiet, soweit dies nach vernünftigem Ermessen für die Erbringung der Serviceleistungen erforderlich ist.

3. Datenschutz-Folgenabschätzung (DSFA).

Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung mit dem Verantwortlichen in angemessener Weise zusammenarbeiten und ihn im erforderlichen Umfang unterstützen, damit dieser seiner Verpflichtung gemäß DSGVO nachkommen kann, eine Datenschutz-Folgenabschätzung in Bezug auf seine Nutzung der Serviceleistungen durchzuführen, insoweit als der Verantwortliche nicht anderweitig auf die betreffenden Informationen zugreifen kann und diese Informationen dem Auftragsverarbeiter zur Verfügung stehen. Der Auftragsverarbeiter unterstützt den Verantwortlichen in angemessener Weise bei der Zusammenarbeit mit oder im Fall einer Anhörung durch die Aufsichtsbehörde zur Erfüllung seiner Aufgaben gemäß Datenschutz-Folgenabschätzung durch den Verantwortlichen, soweit dies nach der DSGVO erforderlich ist.

4. **Rechte betroffener Personen.** Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, soweit gesetzlich zulässig, unverzüglich, wenn er von einer betroffenen Person einen Antrag in Bezug auf die Ausübung ihres Auskunftsrechts und ihrer Rechte auf Berichtigung, Einschränkung der Verarbeitung, Vergessenwerden, Datenübertragbarkeit, Widerspruch bei der Verarbeitung oder ihres Rechts, nicht einer auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, erhält. Der Auftragsverarbeiter hat den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung des Antrags der betroffenen Person nachzukommen.

5. **Beschränkte Nutzung von personenbezogenen Daten und Mitarbeitern.** Soweit im Servicevertrag nicht etwas anderes bestimmt ist, (i) erwirbt der Auftragsverarbeiter keine Rechte an den personenbezogenen Daten und (ii) haben der Auftragsverarbeiter und seine verbundenen Unternehmen angemessene Maßnahmen zu ergreifen, um die Zuverlässigkeit aller Mitarbeiter, Bevollmächtigten oder Auftragnehmer eines beauftragten Unterauftragsverarbeiters, die möglicherweise Zugriff auf die personenbezogenen Daten haben, zu gewährleisten, wobei in jedem Fall sicherzustellen ist, dass der Zugriff strikt auf diejenigen Personen beschränkt wird, die für die Zwecke des Servicevertrags von den jeweiligen personenbezogenen Daten unbedingt Kenntnis haben oder darauf zugreifen müssen, und die geltenden Gesetze zum Datenschutz und Schutz der Privatsphäre einhalten. Dabei ist sicherzustellen, dass alle diese Personen Vertraulichkeitsverpflichtungen oder berufsständischen oder gesetzlichen Verschwiegenheitspflichten unterliegen.

6. **Unterauftragsverarbeiter.**

a. **Ernennung von Unterauftragsverarbeitern.** Der Verantwortliche stimmt dem Einsatz von Unterauftragsverarbeitern durch den Auftragsverarbeiter grundsätzlich zu. Der Verantwortliche nimmt dies zur Kenntnis und stimmt zu, dass (a) die verbundenen Unternehmen des Auftragsverarbeiters als Unterauftragsverarbeiter eingesetzt werden dürfen und (b) der Auftragsverarbeiter und seine verbundenen Unternehmen im Zusammenhang mit der Bereitstellung der Serviceleistungen externe Unterauftragsverarbeiter in Anspruch nehmen können. Der Auftragsverarbeiter oder seine verbundenen Unternehmen haben mit jedem Unterauftragsverarbeiter eine schriftliche Vereinbarung mit Datenschutzverpflichtungen geschlossen, die nicht weniger Schutz bietet als die in diesem Vertrag enthaltenen Verpflichtungen zum Schutz der Daten des Verantwortlichen, soweit diese auf die Art der von diesem Unterauftragsverarbeiter erbrachten Serviceleistungen anwendbar sind. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt.

b. **Liste.** Die aktuelle Liste der Unterauftragsverarbeiter für die Serviceleistungen kann auf der Proofpoint-Trust-Webseite auf https://www.proofpoint.com/us/legal/trust eingesehen werden. Wenn der Auftragsverarbeiter an dieser Liste Änderungen oder Ergänzungen vornimmt, wird der Verantwortliche (sofern er sich auf der Webseite zu Vertrauen für den Benachrichtigungsdienst angemeldet hat) über diese Änderungen per E-Mail benachrichtigt. Die Parteien vereinbaren, dass diese Benachrichtigung die Informationspflicht gemäß Artikel 28 Absatz 2 der DSGVO und Ziffer 9 der Standardvertragsklauseln erfüllt.

c. **Einwände.** Der Verantwortliche kann Einwände gegen den Einsatz eines neuen Unterauftragsverarbeiters erheben, indem er dem Auftragsverarbeiter unverzüglich eine entsprechende schriftliche Mitteilung an privacy@proofpoint.com übermittelt. Falls der Verantwortliche Einwände gegen einen neuen Unterauftragsverarbeiter erhebt, wird der Auftragsverarbeiter (nach Zugang des schriftlichen Widerspruchs gemäß dem vorstehenden Satz) nach vernünftigem Ermessen bestimmen, ob für den Verantwortlichen Anpassungen vorgenommen werden können, um die Verarbeitung personenbezogener Daten durch den beanstandeten neuen Unterauftragsverarbeiter zu vermeiden, ohne den Verantwortlichen übermäßig zu belasten. Ist dem Auftragsverarbeiter eine solche Änderung innerhalb einer angemessenen Frist von höchstens dreißig (30) Tagen nicht möglich, ist der Verantwortliche berechtigt, die entsprechende Bestellung nur in Bezug auf diejenigen Serviceleistungen, die vom Auftragsverarbeiter ohne den Einsatz des beanstandeten neuen Unterauftragsverarbeiters nicht erbracht werden können, innerhalb von dreißig (30) Tagen nach der Entscheidung des Auftragsverarbeiters durch schriftliche Mitteilung an den Auftragsverarbeiter zu kündigen.

7. **Besondere Kategorien personenbezogener Daten.** Der Verantwortliche (und seine verbundenen Unternehmen in der Europäischen Union) trägt die alleinige Verantwortung für die Einhaltung der für ihn (und seine verbundenen Unternehmen in der Europäischen Union) geltenden Gesetze zum Datenschutz und Schutz der Privatsphäre, einschließlich personenbezogener Daten, die eine besondere Behandlung erfordern, oder besonderer Kategorien personenbezogener Daten, darunter Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit einer Person hervorgehen, sowie Gesundheitsdaten, Daten zum Sexualleben oder zu den finanziellen Verhältnissen einer Person.

8. **Sicherheit personenbezogener Daten.**

a. Um die Sicherheit personenbezogener Daten zu gewährleisten, hat der Auftragsverarbeiter mindestens die technischen und organisatorischen Maßnahmen in Anhang 2 umzusetzen. Hierzu gehören der Schutz personenbezogener Daten vor einer Sicherheitsverletzung, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung.

b. Der Auftragsverarbeiter gewährt seinen Mitarbeitern nur insoweit Zugriff auf derzeit in Verarbeitung befindende personenbezogene Daten, als dies für die Durchführung, Verwaltung und Überwachung des Servicevertrags erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die Personen, die zur Verarbeitung der erhaltenen personenbezogenen Daten befugt sind, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

9. **Zusammenarbeit mit den Aufsichtsbehörden.** Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung seiner Aufgaben gemäß Ziffer 8 dieses Vertrags unterstützen. Außerdem unternimmt der Auftragsverarbeiter im Zusammenhang mit einem aufsichtsbehördlichen Ersuchen auf Kosten des Verantwortlichen zumutbare Anstrengungen, um die angemessene Zusammenarbeit und Unterstützung von Unterauftragsverarbeitern bei der Bereitstellung des Zugangs zu zweckdienlichen Informationen, die zur Erfüllung der Pflichten des Verantwortlichen gemäß der DSGVO notwendig sind, zu erwirken.

10. **Verletzung des Schutzes personenbezogener Daten.**

a. Im Falle der Kenntniserlangung einer unbefugten Nutzung, Offenlegung oder Beschaffung personenbezogener Daten durch Dritte, die die Sicherheit, Vertraulichkeit oder Integrität der vom Auftragsverarbeiter verwalteten personenbezogenen Daten beeinträchtigt („Sicherheitsverletzung“), wird der Auftragsverarbeiter den Verantwortlichen innerhalb von 48 Stunden schriftlich über die Verletzung in Kenntnis setzen und ihn danach regelmäßig über den weiteren Fortgang auf dem Laufenden halten.

b. Diese Mitteilung enthält zumindest folgende Angaben:
   (i) eine Beschreibung der Art der Sicherheitsverletzung (soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und betroffenen Datensätze);
   (ii) die Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können; und
   (iii) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Sicherheitsverletzung, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

c. Wenn und soweit nicht sämtliche dieser 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, unverzüglich bereitgestellt.

11. **Internationale Datenübermittlung.**

a. **Allgemeine Bestimmungen.** Der Auftragsverarbeiter befolgt die Vorschriften geltender Datenschutzgesetze hinsichtlich der Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum ins Ausland. Personenbezogene Daten dürfen ausschließlich zur Erbringung von

Serviceleistungen für den Verantwortlichen gemäß Servicevertrag in Länder, einschließlich Drittländern, in denen der Auftragsverarbeiter oder seine Unterauftragsverarbeiter tätig sind, übermittelt und dort gespeichert und/oder verarbeitet werden. Jede Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum unterliegt den Standardvertragsklauseln, die die Parteien hiermit abschließen und in diesem Vertrag als Anlage 2 enthalten sind.

b. **Datentransfer-Folgenabschätzung.** Bei einigen Sicherheitsdiensten des Auftragsverarbeiters ist es erforderlich, dass eine gewisse Menge an personenbezogenen Daten in die Vereinigten Staaten übertragen wird. Im Hinblick auf Klausel 14 Absatz b der Standardvertragsklauseln hat der Auftragsverarbeiter eine Datentransfer-Folgenabschätzung (sog. „Data Transfer Assessment", auch als „Transfer Impact Assessment" bezeichnet) erstellt, die unter https://www.proofpoint.com/sites/default/files/misc/pfpt-us-data-transfer-assessment-20201028.pdf abgerufen werden kann.

12. Behördliche Auskunftsersuche.

a. Gemäß Klausel 15 der Standardvertragsklauseln wird der Auftragsverarbeiter keine Kundendaten gegenüber Dritten offenlegen, es sei denn, eine solche Offenlegung ist jeweils zur Aufrechterhaltung oder Erbringung der Serviceleistungen oder zur Einhaltung gesetzlicher Vorschriften oder einer gültigen und verbindlichen Anordnung vonseiten einer staatlichen Stelle (wie eine Vorladung oder gerichtliche Verfügung) notwendig. Wenn der Auftragsverarbeiter von einer staatlichen Stelle ein Ersuchen zur Offenlegung sensibler Daten des Verantwortlichen erhält, wird der Auftragsverarbeiter die staatliche Stelle an den Verantwortlichen weiterverweisen, damit die Daten direkt bei diesem angefordert werden können. Dabei kann der Auftragsverarbeiter der staatlichen Stelle wesentliche Kontaktdaten des Verantwortlichen zur Verfügung stellen. Wenn der Auftragsverarbeiter gezwungen ist, Daten des Verantwortlichen an eine staatliche Stelle weiterzugeben, wird er den Verantwortlichen in angemessener Weise über die Forderung unterrichten, um diesem die Möglichkeit zu geben, eine einstweilige Verfügung oder ein anderes geeignetes Rechtsmittel zu beantragen, es sei denn, dem Auftragsverarbeiter ist dies gesetzlich untersagt. Gemäß dem US-amerikanischen Foreign Intelligence Surveillance Act (FISA) ist der Auftragsverarbeiter ein Remote-Computing-Dienstleister und kein Telekommunikationsanbieter; daher ist es (nach Einschätzung des Auftragsverarbeiters) unwahrscheinlich, dass das Unternehmen Gegenstand staatlicher Auskunftsersuche nach solchen Rechtsvorschriften wird.

b. Um sicherzustellen, dass sich der Verantwortliche der Risiken bewusst wird und bleibt, die mit der Übermittlung von Daten in ein Drittland verbunden sind, kann der Auftragsverarbeiter von Zeit zu Zeit auf angemessenes Ersuchen vonseiten des Verantwortlichen, jedoch höchstens einmal pro Kalenderjahr, einen strukturierten Fragebogen über die Gesetze und Vorschriften im Bestimmungsland beantworten, die auf den Auftragsverarbeiter oder seine Unterauftragsverarbeiter anwendbar sind und die den Behörden den Zugang zu den Daten des Verantwortlichen, die Gegenstand der Übermittlung sind, ermöglichen würden, insbesondere in den Bereichen Nachrichtendienst, Strafverfolgung sowie Verwaltungs- und Aufsichtsbehörden, die für die übermittelten Daten gelten. Der Auftragsverarbeiter muss in der Lage sein, dem Verantwortlichen diese Art von Informationen nach bestem Wissen und Gewissen zur Verfügung zu stellen, nachdem er sich nach Kräften bemüht hat, diese Informationen zu erhalten.

13. Verifizierung und Prüfung.

a) Gemäß Artikel 28 Absatz 3 Buchstabe h der DSGVO hat der Auftragsverarbeiter dem Verantwortlichen auf begründete schriftliche Anfrage und vorbehaltlich der Unterzeichnung einer gesonderten Geheimhaltungsvereinbarung Informationen über die Verarbeitung personenbezogener Daten des Verantwortlichen als Nachweis für die Einhaltung der Pflichten des Auftragsverarbeiters aus diesem Vertrag zur Verfügung zu stellen. Der Auftragsverarbeiter kommt in folgenden Fällen dem Antrag des Verantwortlichen oder eines unabhängigen Prüfers zur Durchführung von Prüfungen vor Ort im Zusammenhang mit der Verarbeitung personenbezogener Daten nach, um die Einhaltung dieses Vertrags durch den Auftragsverarbeiter zu verifizieren: (a) wenn der Auftragsverarbeiter keine ausreichenden schriftlichen Nachweise für seine Einhaltung der technischen und organisatorischen Maßnahmen vorgelegt hat; (b) wenn eine Sicherheitsverletzung eingetreten ist; (c) wenn eine Prüfung von der Aufsichtsbehörde des Verantwortlichen offiziell angeordnet wird oder (d) wenn in Datenschutzgesetzen ein obligatorisches Recht des Verantwortlichen zur Durchführung von Vor-Ort-Prüfungen vorgesehen ist; mit der Maßgabe, dass der Verantwortliche dieses Recht nicht häufiger als einmal jährlich ausübt, sofern Datenschutzgesetze nicht zwingend einen häufigeren Prüfungsturnus vorschreiben. Alle gemäß dieser Ziffer von dem Auftragsverarbeiter zur Verfügung gestellten

Informationen und/oder durchgeführten Prüfungen stehen unter dem Vorbehalt der Unterzeichnung einer gesonderten Geheimhaltungsvereinbarung. Derartige Vor-Ort-Prüfungen sind in einer Weise durchzuführen, die die laufende Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit, den unterbrechungsfreien Betrieb und die Belastbarkeit der geprüften Einrichtungen nicht beeinträchtigt und die dort verarbeiteten vertraulichen Daten keinen anderweitigen Risiken oder Gefährdungen aussetzt.

b) Jede Partei trägt die eigenen Kosten im Zusammenhang mit einer Prüfung oder Inspektion. Dies gilt auch für die Bereitstellung von Informationen oder Prüfungen nach Maßgabe von Klausel 8.9 Buchstaben c bis e der Standardvertragsklauseln.

14. Beendigung.

Der Verantwortliche bestätigt und stimmt zu, dass im Falle einer Aussetzung oder Beendigung der Datenverarbeitung gemäß diesem Vertrag oder Klausel 18 der Standardvertragsklauseln die Fristen für die Einstellung der gesamten Verarbeitung und Löschung personenbezogener Daten durch den Auftragsverarbeiter durch den Servicevertrag geregelt werden.

ANHANG 1 ZUM VERTRAG – EINZELHEITEN DER VERARBEITUNG

Der vorliegende Anhang 1 enthält bestimmte Angaben zur Verarbeitung personenbezogener Daten des Kunden gemäß den Bestimmungen in Artikel 28 Absatz 3 der DSGVO (bzw. entsprechenden Bestimmungen anderer Datenschutzgesetze).

Produkt	Betroffene Personen	Kategorien von verarbeiteten personenbezogenen Daten	Verarbeitungsvorgänge	Aufbewahrungsfrist
Archive	Mitarbeiter, Auftragnehmer und Kunden	Alle personenbezogenen Daten, die in erfassten Inhalten enthalten sind (einschließlich E-Mails, Sofortnachrichten, Inhalte sozialer Medien, zugehörige Nachrichtentelemetrie und Anhänge)	Archive ist eine Cloud-basierte Archivierungslösung, die für die juristische Aufdeckung, die Einhaltung gesetzlicher Vorschriften und den Datenzugriff für die Endnutzer des Kunden entwickelt wurde und ein zentrales, durchsuchbares Repository bietet, das eine Vielzahl von Inhaltstypen unterstützt.	Wie vom Verantwortlichen festgelegt
CAD/CASB	Mitarbeiter, Auftragnehmer	Metadaten von Cloud-Kontoinhabern (E-Mail-Adressen, Namen, Position), Datei-Metadaten und Zugriffsprotokolle der Cloud-Konten	Cloud Account Defense hilft dem Kunden, verdächtige Aktivitäten rund um die Cloud-Konten des Kunden zu erkennen und kompromittierte Cloud-Konten zu identifizieren. Cloud App Security Broker verwendet Richtlinien, um den Verlust sensibler oder vertraulicher Daten des Kunden zu verhindern, die in den Cloud-Konten des Kunden enthalten sind. CASB IaaS Protection unterstützt den Kunden bei der Identifizierung seiner IaaS-Ressourcen, dem Schutz sensibler Daten innerhalb des IaaS-Speichers und der Überwachung und Unterbindung unbefugter Anmeldungen auf den Cloud-Konten des Kunden	Bis zu 180 Tage ab dem Ende des Abonnements des Verantwortlichen
Cloudmark Active Filter, Authority, Content Categories, Insight Server und Sender Intelligence; Cloudmark Spam Reporting Service	Mitarbeiter, Auftragnehmer und Kunden	Telemetriedaten in Verbindung mit E-Mails, SMS-, MMS- und RCS-Nachrichten, einschließlich E-Mail-Adressen, IP-Adressen und Telefonnummern	Cloudmark-Produkte nutzen intelligente Bedrohungsanalysen, um E-Mail und Mobile Messaging vor Spam und Malware zu schützen.	30 Tage bei Nachrichten, die vom Empfänger als potenziell schädlich gemeldet wurden. 30 Tage bei Nachrichten, die vom Empfänger als unschädlich eingestuft wurden.
Cloudmark Safe Messaging Cloud, Cloudmark Safe Messaging Cloud Hybrid	Mitarbeiter, Auftragnehmer und Kunden	Telemetriedaten in Verbindung mit E-Mails, SMS-, MMS- und RCS-Nachrichten, einschließlich E-Mail-Adressen, IP-Adressen und Telefonnummern	Cloudmark-Produkte nutzen intelligente Bedrohungsanalysen, um E-Mail und Mobile Messaging vor Spam und Malware zu schützen.	30 Tage bei Nachrichten, die vom Empfänger als potenziell schädlich gemeldet wurden. 30 Tage bei Nachrichten, die vom Empfänger als unschädlich eingestuft wurden. Ansonsten wie vom Verantwortlichen ausgehandelt.

Compliance Gateway	Mitarbeiter, Auftragnehmer und Kunden	Alle personenbezogenen Daten, die in erfassten Inhalten enthalten sind (einschließlich E-Mails, Sofortnachrichten, Inhalte sozialer Medien, zugehörige Nachrichtenteletrie und Anhänge)	Compliance Gateway fungiert als zentraler Knotenpunkt für das Filtern und Weiterleiten von Nachrichteninhalten an die Archiv-, Überwachungs- und Analysesysteme des Kunden.	Bis zu 14 Tage nach Ablauf des Abonnements des Verantwortlichen
Content Capture	Mitarbeiter, Auftragnehmer und Kunden	Alle personenbezogenen Daten, die in erfassten Inhalten enthalten sind (einschließlich E-Mails, Sofortnachrichten, Inhalte sozialer Medien, zugehörige Nachrichtenteletrie und Anhänge)	Content Capture erfasst Inhalte von unterstützten Messaging- und Cloud-Speicherplattformen und stellt sie für Compliance-Dienste wie E-Discovery, Archivierung und Überwachung bereit.	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen
Content Patrol	Mitarbeiter, Auftragnehmer und Kunden	Alle personenbezogenen Daten, die in erfassten Inhalten enthalten sind (einschließlich E-Mails, Sofortnachrichten, Inhalte sozialer Medien, zugehörige Nachrichtenteletrie und Anhänge)	Content Patrol ermöglicht es Kunden, die Aktivitäten der Endbenutzer auf den von kontrollierten Social-Media-Konten zu erfassen, zu überwachen, zu korrigieren und Compliance-Berichte zu erstellen.	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen
Continuity	Mitarbeiter, Auftragnehmer und alle anderen Personen, die E-Mails über das E-Mail-System des Verantwortlichen senden oder empfangen	Alle in einer E-Mail enthaltenen personenbezogenen Daten	Continuity bietet eine temporäre Speicherung von ein- und ausgehenden Kunden-E-Mails innerhalb der webbasierten On-Demand-E-Mail. Continuity dient nur als sekundäre Failover-Option für den Fall, dass der E-Mail-Dienst des Kunden ausfällt, und nicht als primäre E-Mail-Archivierungslösung oder primäre Failover-Lösung	Nachrichten verfallen nach 30 Tagen.
Digital Discover, Digital Protection und Digital Compliance	Mitarbeiter, Auftragnehmer, Kunden oder andere Personen, die auf den Social-Media-Konten des Kunden posten	IDs geschäftlicher Social-Media-Benutzerkonten, Social-Media-Inhalte und optionale biografische Angaben, sofern im Kontoprofil der geschäftlichen Nutzer enthalten	Scannen von Social-Media-Plattformen auf mit einem Kunden verbundenen Konten, um falsche, betrügerische und verleumderische Konten zu ermitteln, die mit dem Kunden im Zusammenhang stehen. Analyse von statischen und interaktiven Inhalten. Schnittstellen zum Archivierungsdienst für soziale Medien, wie für Compliance-Zwecke erforderlich.	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen
Email Data Loss Prevention (DLP)	Mitarbeiter, Auftragnehmer und alle anderen Personen, die über das E-Mail-System des Kunden E-	Alle in einer E-Mail enthaltenen personenbezogenen Daten	E-Mail-DLP setzt Richtlinien ein, um den Verlust sensibler oder vertraulicher Daten des Kunden per E-Mail zu verhindern.	Bis zu 366 Tage nach der Erfassung, mit Ausnahme von Threat Analytics, die bis zu 18 Monate nach der Erfassung aufbewahrt werden.

	Mails senden oder empfangen			
Email Fraud Defense	Mitarbeiter, Auftragnehmer, Kunden und alle anderen Personen, die E-Mails über das E-Mail-System des Unternehmens des Kunden senden oder empfangen	Informationen im E-Mail-Header, wie E-Mail-Adressen, IP-Adressen, Namen des Absenders und Empfängers	EFD verarbeitet bereichsbezogene Nachrichtenauthentifizierung, Berichterstattung und Konformität (DMARC) aggregierte Berichte und forensischen DMARC-Nachrichtenmusterverkehr für Kundendomänen und bewertet die Authentizität von Absendern auf der Grundlage von Absender-Authentifizierungsdaten, um von nicht authentifizierten und nicht autorisierten Quellen stammenden Verkehr hervorzuheben.	Die forensischen Daten von Cloudmark werden nach der Erfassung 30 Tage lang aufbewahrt. DMARC-Forensikdaten werden nach der Erfassung 90 Tage lang aufbewahrt.
Email Encryption	Mitarbeiter, Auftragnehmer, Kunden und alle anderen Personen, die E-Mails über das E-Mail-System des Unternehmens des Kunden senden oder empfangen	Alle in einer E-Mail enthaltenen personenbezogenen Daten	Email Encryption bietet eine vollständig integrierte Lösung zur Ver- und Entschlüsselung von Nachrichten.	Der Inhalt der verschlüsselten Nachricht wird nach Maßgabe des Verantwortlichen aufbewahrt (bis zu 366 Tage).
E-Mail-Protection	Mitarbeiter, Auftragnehmer und alle anderen Personen, die E-Mails über das E-Mail-System des Verantwortlichen senden oder empfangen	Alle in einer E-Mail enthaltenen personenbezogenen Daten	Der E-Mail-Protection umfasst Funktionen wie Spam-Erkennung zur Identifizierung und Klassifizierung von Spam-Nachrichten; Virenschutzfunktionen zur Erkennung und Filterung von Nachrichten mit bekannten Viren; Zero-Hour-Antivirus-Funktionen zur Erkennung und Filterung von Nachrichten mit verdächtigen Inhalten; Quarantäne-Ordner zur Analyse und Beseitigung verdächtiger Inhalte	Bis zu 18 Monate nach der Erfassung
Endpoint Data Loss Prevention	Mitarbeiter, Auftragnehmer	Erfasste Metadaten für die Benutzer des Verantwortlichen	Endpoint Data Loss Prevention setzt Software (einen Agenten) auf kundeneigenen oder kontrollierten Desktops und Servern auf unterstützten Plattformen ein. Diese Agenten erfassen Metadaten, die von den Aktivitäten lizenzierter Benutzer aufgezeichnet werden, und speichern diese Daten im Endpoint-Data-Loss-Prevention-Archiv von Proofpoint.	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen
Essentials	Mitarbeiter, Auftragnehmer und Kunden	Alle in einer E-Mail enthaltenen personenbezogenen Daten	Scannen, Filtern und Routing während der Übertragung von E-Mails an und von externen Parteien des Kunden über das geschäftliche E-Mail-System des Kunden. Wenn die Archivierungsfunktion verwendet wird, siehe „Archive“ weiter oben Wenn TAP-Sandboxing verwendet wird, siehe TAP weiter unten	Bis zu 18 Monate nach der Erfassung.
Insider Threat Management SaaS	Mitarbeiter, Auftragnehmer: a) ITM SaaS-Administratoren oder Analysten, die das Webportal nutzen	E-Mail-Adresse, Gerätekennung wie IP-Adresse, Benutzerinformationen wie Name und Benutzer-ID, Website-Informationen wie URL und Seitenname, Anwendungsinformationen wie	ITM setzt auf festgelegten Laptop-, Desktop- und Servergeräten, die sich im Eigentum des Verantwortlichen befinden oder von diesem gesteuert werden, einen Endpoint Agent ein. Die Agenten erfassen Telemetriedaten über die Aktivitäten der Gerätenutzer, der betroffenen Personen. Wenn die Funktion vom Verantwortlichen aktiviert wird, können die Agenten auch Screenshots von den Aktivitäten auf den Geräten der Nutzer aufnehmen. Die Aktivierung der Screenshot-Funktion und	In Übereinstimmung mit der vom Verantwortlichen gewählten Aufbewahrungsfrist bis zu einer Höchstdauer von 366 Tagen.

	b) Endpunktbenutzer, die die Endpunkte des Datenexporteurs verwenden, auf denen der ITM SaaS-Agent installiert ist	Anwendungsname, Name der ausführbaren Datei und Fenstertitel. Außerdem kann mit ITM der Bildschirminhalt gespeichert werden; diese Funktion wird vom Kunden konfiguriert und gesteuert. Die Bildschirmaufnahme könnte zusätzliche personenbezogene Daten enthalten, die auf dem Benutzerbildschirm angezeigt werden.	die Dauer der Datenspeicherung dieser Inhalte liegt im alleinigen Ermessen des Kunden. Die Telemetrie- und Screenshot-Daten werden im mehrinstanzenfähigen ITM SaaS-Speicher gespeichert.	
Intelligent Classification and Protection	Mitarbeiter, Auftragnehmer, Kunden und alle Personen, die das Dokument einsehen.	Alle in einem Dokument enthaltenen personenbezogenen Daten.	Automatisches Auffinden und Identifizieren sensibler und geschäftskritischer Daten zur Verbesserung bestehender Datenschutzlösungen wie Kennzeichnung, Verschlüsselung, Zugriffskontrolle, Schutz vor Datenverlust, CASB und Vorschläge für Schutzregeln und/oder -richtlinien für den Kunden	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen
Internal Mail Defense (IMD)	Mitarbeiter, Auftragnehmer	Alle in einer E-Mail enthaltenen personenbezogenen Daten	IMD setzt E-Mail-Schutz- und TAP-Funktionen ein, um die interne E-Mail-Kommunikation des Kunden vor Spam und bösartigen Inhalten zu schützen.	Bis zu 18 Monate nach der Erfassung.
Browser and E-mail Isolation	Mitarbeiter und Auftragnehmer	E-Mail-Adressen, Cookies auf Benutzersites und Browserverlauf sowie Rechenzentrumsstandort des Containers mit isolierten Inhalten	Die Produkte zur Browser- und E-Mail-Isolation richten eine isolierte Remote-Webbrowser- oder Web-E-Mail-Umgebung ein, um den Kunden vor potenziellen Bedrohungen zu schützen, wenn Benutzer über kundeneigene Geräte oder die Geräte des Verantwortlichen eine Verbindung mit dem Internet oder webbasierten E-Mail-Konten herstellen. Der Kunde wird den Benutzern nicht gestatten, über Isolation verletzendes, verleumderisches, bedrohliches oder beleidigendes Material zu übermitteln (oder auf Isolation zu veröffentlichen).	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen
NexusAI for Compliance	Mitarbeiter, Auftragnehmer und Kunden	Alle personenbezogenen Daten, die in den erfassten Inhalten enthalten sind (einschließlich E-Mails, Sofortnachrichten, Inhalte sozialer Medien, zugehörige Nachrichtentelemetrie und Anhänge)	NexusAI for Compliance nutzt maschinelles Lernen, um unterstützte archivierte Nachrichten (wie E-Mails, soziale Medien, Kollaborationsplattformen und mobile Nachrichten) auszuwerten, die von Proofpoints Intelligent Supervision zur Überprüfung durch den Kunden markiert wurden.	Bis zu 24 Stunden nach dem Ende des Abonnements des Verantwortlichen
Nexus People Risk Explorer	Mitarbeiter, Auftragnehmer	Namen, E-Mail-Adressen und alle in Threat Analytics enthaltenen personenbezogenen Daten	Proofpoint Nexus People Risk Explorer nutzt personenbezogene Sicherheitsdaten aus Targeted Attack Protection, Security Awareness Training, Cloud Account Defense und Cloud Account Security Broker von Proofpoint, um Einblicke in die Art, Schwere und Häufigkeit von Bedrohungen zu geben, die auf den Kunden und seine Mitarbeiter abzielen.	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen

Anti-Phishing Suite: enthält PhishAlarm und PhishAlarmAnalyzer:	Mitarbeiter, Auftragnehmer	Name E-Mail Adresse Alle in einer E-Mail enthaltenen personenbezogenen Daten	Weiterleitung und Scannen verdächtiger E-Mails, die von Endbenutzern über die Schaltfläche „PhishAlarm“ gemeldet werden. PhishAlarm Analyzer bietet eine reaktionsschnelle Identifizierung von Phishing-Angriffen in Echtzeit. Die über PhishAlarm und PhishAlarm Analyzer gemeldeten E-Mails werden abgerufen und kategorisiert und stehen den zuständigen Teams des Kunden sofort zur Verfügung.	Bis zu 30 Tage nach dem Ende des Abonnements des Verantwortlichen; mit Ausnahme von Threat Analytics, wo eine Aufbewahrung von bis zu 18 Monaten nach der Erfassung gilt
Proofpoint Security Awareness Training (PSAT)	Mitarbeiter, Auftragnehmer	Name, E-Mail-Adresse und weitere Datenfelder, die der Kunde zum Hochladen aus seinem Active Directory in PSAT ausgewählt hat	Die personenbezogenen Daten werden zur Durchführung des Mitarbeiter-Cybersicherheitstrainings und für die mitarbeiterbezogenen Sicherheitsbeurteilungen und Berichte verwendet.	Maximal 90 Tage ab dem Ende des Abonnements des Verantwortlichen; während des Abonnements de Verantwortlichen können dessen Administratoren jedoch Änderungen an Benutzern vornehmen und diese löschen.
Secure E-Mail Relay (SER)	Mitarbeiter Auftragnehmer Alle Empfänger von Massen-E-Mails, die über das firmeneigene E-Mail-System des Kunden verschickt werden	Name E-Mail Adresse Alle in einer E-Mail enthaltenen personenbezogenen Daten	SER ist eine gehostete, mehrmandantenfähige Lösung, die dem Kunden die Kontrolle über Anwendungen gibt, die E-Mails über kundeneigene oder vom Kunden kontrollierte Domains versenden. Jede Anwendung erhält eine zusätzliche Sicherheitsebene und verteilt die E-Mails nach der Durchführung von Proofpoint AS/AV-Prüfungen DMARC-konform an das Internet. SER darf nur für die Zustellung von E-Mails verwendet werden, die den geltenden Gesetzen über Massenversand oder unerwünschte Nachrichten entsprechen.	Bis zu 30 Tage ab dem Ende des Abonnements des Verantwortlichen
SecureShare	Mitarbeiter, Auftragnehmer sowie jede andere Person, an die eine Datei freigegeben wurde	Name, E-Mail-Adressen	SecureShare ist eine sichere Methode für die Freigabe von Dateien und die vorübergehende Speicherung solcher Dateien.	Bis zu 180 Tage nach der Erfassung.
Targeted Attack Protection (TAP)	Mitarbeiter, Auftragnehmer und Kunden Jede andere Person, die E-Mails über das E-Mail-System des Unternehmens des Kunden sendet oder empfängt	Name E-Mail Adresse Alle in einer E-Mail enthaltenen personenbezogenen Daten	TAP identifiziert und schützt mithilfe einer dynamischen Malware-Analyse-Engine vor bösartigen URLs und E-Mail-Anhängen.	Bis zu 18 Monate nach der Erfassung.
Threat Response Cloud (“TRC”)	Mitarbeiter, Auftragnehmer und Kunden Jede andere Person, die E-Mails über das E-Mail-System des Unternehmens des Kunden sendet oder empfängt	Name E-Mail Adresse Alle in einer E-Mail enthaltenen personenbezogenen Daten	TRC ist eine Plattform zur Verwaltung von Vorfällen, die eine Automatisierung zur Analyse und Entfernung unerwünschter E-Mails beinhaltet.	Die Länge der Aufbewahrung von abgeschlossenen Vorfällen wird vom Verantwortlichen festgelegt. Bei abgeschlossenen Vorfällen werden die vollständigen MIME-Daten alle 30 Tage gelöscht.
ThreatSimulator	Mitarbeiter, Auftragnehmer	Name E-Mail Adresse	Personenbezogene Daten werden für simulierte Phishing-Kampagnen verwendet.	Auf Anfrage des Kunden und innerhalb

			Der Kunde darf nur simulierte Phishing-E-Mails an Domänen senden, die dem Kunden gehören oder von diesem kontrolliert werden.	von 90 Tagen nach einer solchen Anfrage.
Zero Trust Network Access (vormals: Meta)	Mitarbeiter, Auftragnehmer	E-Mail-Adresse und Name (und optional: Telefonnummer) des Benutzers und Ereignisse, die den Intranetverkehr betreffen, wie „Zulassen“/„Ablehnen“-Ereignisse und DNS-Abfragen (der Kunde kann die Protokollierung von Ereignissen, die den Internetverkehr betreffen, aktivieren oder deaktivieren)	Meta ist als Zero-Trust-Networkauf dem Firmennetzwerk des Kunden aufgesetzt. Die Benutzer greifen auf das Firmennetzwerk zu, indem sie sich über ein VPN mit ihren Anmeldedaten mit der Meta-Netzwerkschicht verbinden. Nach der Anmeldung im Meta-Netzwerk wird jedem Benutzer eine eindeutige Identität zugewiesen, mit der eine Verbindung zum darunterliegenden Firmennetzwerk des Datenexporteurs hergestellt wird.Der Zugriff auf die Assets innerhalb des Firmennetzwerk des Datenexporteurs erfolgt auf Basis der eindeutigen Identität des Benutzers.	Bis zu 90 Tage ab dem Ende des Abonnements des Verantwortlichen

1. Unterauftragsverarbeiter

Eine aktuelle Liste der Unterauftragsverarbeiter kann unter https://www.proofpoint.com/us/legal/trust abgerufen werden.

ANHANG 2 ZUM VERTRAG – SICHERHEIT BEI DER VERARBEITUNG

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter die nachstehenden Maßnahmen, um ein angemessenes Schutzniveau bei der Bereitstellung der Serviceleistungen zu gewährleisten:

A. *Benutzerauthentifizierung*

Die Geschäftsleitung hat ein Informationssicherheitsprogramm ausgearbeitet und beschlossen.
Es wurde ein Rahmen von Richtlinien und Normen für die Informationssicherheit im Sinne der Ziele des Informationssicherheitsprogramms entwickelt.
Es gibt Verfahren für die Authentifizierung und Autorisierung von Nutzern für den Zugriff auf Systeme und die Einhaltung der diesbezüglichen Regeln.
Es gibt Verfahren für die Anforderung, Festlegung, Einrichtung, vorübergehende Sperrung, Löschung und Schließung von Benutzerkonten und der zugehörigen Zugriffsrechte und die Einhaltung der diesbezüglichen Richtlinien. Beispielsweise wird der Systemzugriff der Rolle entsprechend und auf dem Prinzip der geringsten Rechte (Least-Privilege-Prinzip) erteilt.
Es ist ein Prozess zur Überwachung fehlgeschlagener Anmeldeversuche installiert. Festgestellte Sicherheitsverletzungen werden behoben.
Der Zugriff auf die Produktionsumgebung des Auftragsverarbeiters durch dessen Mitarbeiter wird auf der Grundlage geschäftlicher Erfordernisse gewährt. Es wird ein VPN mit Zwei-Faktor-Authentifizierung verwendet.
Für Änderungen in der Produktionsumgebung wurden Kontrollen eingerichtet, die solche Änderungen nur auf berechtigte Personen beschränken.

Zugriffsart

Die verschiedenen Arten des Zugriffs von Endnutzern des Kunden sind im servicespezifischen Administratorhandbuch dokumentiert und werden von den Administratoren des Kunden über das Service-Dashboard, die Benutzeroberfläche oder SAML-Integration gesteuert.

B. *Ausführung von Sicherungskopien*

Die Konfigurations- und Berichtsdaten des Kunden werden regelmäßig gesichert und auf einer Festplatte gespeichert.

Die Verfahren für die Sicherung und Speicherung von Daten und Programmen sind dokumentiert und umgesetzt.

C. *Computer und Zugangsterminals*

Computer, die von Mitarbeitern des Auftragsverarbeiters für den Zugriff auf dessen Infrastruktur verwendet werden, müssen einen sicheren VPN-Tunnel für den Zugriff auf diese verwenden. Auf allen Endgeräten von Mitarbeitern muss eine aktuelle Virenschutzsoftware ausgeführt werden, und die auf diesen Rechnern installierbare Software muss durch entsprechende Richtlinien beschränkt werden. Alle Mitarbeiter des Auftragsverarbeiters sind verpflichtet, sich für den Zugriff auf dessen Unternehmens- und Produktionsnetzwerke bei einem zentralen Authentifizierungssystem zu authentifizieren.

Kontrollen des Datenverarbeiters

Neue Mitarbeiter sind verpflichtet, eine Geheimhaltungsvereinbarung in Bezug auf proprietäre Software und die Vertraulichkeit von Kundeninformationen zu unterzeichnen.
Neue Mitarbeiter erhalten zudem ein Exemplar des Sicherheitskodexes des Auftragsverarbeiters sowie eine Zusammenfassung des Informationssicherheitsprogramms des Auftragsverarbeiters, dessen Erhalt sie bestätigen müssen.

Der Zugriff auf die Produktionsumgebung des Auftragsverarbeiters durch dessen Mitarbeiter wird auf der Grundlage geschäftlicher Erfordernisse gewährt. Es wird ein VPN mit Zwei-Faktor-Authentifizierung verwendet.
Zentralisierte Konfigurationsmanagement-Tools werden verwendet, um sicherzustellen, dass die Endgeräte der Mitarbeiter angemessen konfiguriert sind.

D. ***Zugriffsprotokolle***

Im Zusammenhang mit den Diensten gibt es mindestens zwei Arten von Zugriffsprotokollen:

Alle Zugriffsversuche auf die Computersysteme des Datenverarbeiters werden zentral protokolliert, und ungewöhnliche Aktivitäten werden automatisch der Gruppe für globale Informationssicherheit des Datenverarbeiters gemeldet. Darüber hinaus setzt der Auftragsverarbeiter Richtlinien zur Kontosperrung und Passwortanforderungen durch. Es werden Protokolle über den Kundenzugriff auf die Dienste erstellt und aufbewahrt, soweit dies für die einzelnen Dienste gilt.

Es gibt Verfahren für die Authentifizierung und Autorisierung von Nutzern für den Zugriff auf Systeme und die Einhaltung der diesbezüglichen Regeln.
Ein Kontrollprozess zur regelmäßigen Überprüfung und Bestätigung, dass die Zugriffsrechte weiterhin autorisiert und angemessen sind, ist installiert und wird befolgt.
Es ist ein Prozess zur Überwachung fehlgeschlagener Anmeldeversuche installiert. Festgestellte Sicherheitsverletzungen werden untersucht und behoben.
Die Daten über Anwendungsereignisse werden gespeichert, um chronologische Daten und Protokolle festzuhalten, die eine Überprüfung, Untersuchung und Rekonstruktion von Systemen und Datenverarbeitungs- und Anwendungsereignissen ermöglichen.

E. ***Telekommunikationssysteme***

Alle Produktionsumgebungen des Auftragsverarbeiters verfügen über redundante Internet-Zugänge von verschiedenen Bandbreitenanbietern.

F. ***Mitarbeiterunterweisung***

Alle Mitarbeiter des Auftragsverarbeiters müssen jährlich ein Online-Schulungsprogramm zur Sicherheit und Sensibilisierung absolvieren. Darüber hinaus kann das Personal je nach seiner Funktion fortlaufende Schulungen erhalten. Diese Schulungen können von Proofpoint oder anderen externen Unternehmen durchgeführt werden.

Der Auftragsverarbeiter verfügt über einen Organisationsplan, der die Trennung unvereinbarer Funktionen und Aufgaben betroffener Mitarbeiter sicherstellt.
Es wurden separate Managementfunktionen und Zuständigkeiten festgelegt, um Computerbetrieb, Systementwicklung, Wartung/Instandhaltung und allgemeine Unternehmensfunktionen des Auftragsverarbeiters voneinander zu trennen.
Die Funktionen und Verantwortlichkeiten der Mitarbeiter sind genau definiert.

G. ***Computernutzung***

Der Fernzugriff auf die Produktionsnetze des Auftragsverarbeiters ist auf Systeme beschränkt, auf denen eine von diesem genehmigte und verwaltete Sicherheitssoftware läuft. Alle dem Personal zur Verfügung gestellten Systeme des Auftragsverarbeiters werden über ein zentrales Konfigurationssystem verwaltet. Alle Mitarbeiter des Auftragsverarbeiters werden auf dessen Richtlinien zur zulässigen Nutzung von Computern, Internetzugang und E-Mail-Kommunikation hingewiesen. Die Mitarbeiter des Auftragsverarbeiters müssen diese Richtlinien anerkennen und sich zu deren Einhaltung verpflichten.

Neue Mitarbeiter sind verpflichtet, eine Geheimhaltungsvereinbarung in Bezug auf proprietäre Software und die Vertraulichkeit von Kundeninformationen zu unterzeichnen.
Neue Mitarbeiter lesen und bestätigen den Sicherheitsverhaltenskodex des Auftragsverarbeiters.

H. ***Drucken von Daten***

Kundendaten werden im Speicher verarbeitet und können nicht ausgedruckt werden. Darüber hinaus sind in den Produktionsumgebungen des Auftragsverarbeiters keine Drucker verfügbar, und sämtliche Druckdienste sind auf allen Produktionsservern standardmäßig deaktiviert.

K. ***Physische Zutrittskontrolle***

Kontrollen des Datenverarbeiters

Bei Produkten, die von den Co-Location-Anbietern des Auftragsverarbeiters gehostet werden, kontrolliert der Auftragsverarbeiter den physischen Zugang zu

L.

dessen Infrastruktur. Bei Produkten, die von den Hostinganbietern AWS, Azure oder Google Cloud gehostet werden, erfolgt die physische Zutrittskontrolle durch den Hostinganbieter.

M. Physische Sicherheitsmaßnahmen für Rechenzentren

Die physischen Sicherheitskontrollen der Co-Location-Einrichtungen entsprechen den Standards für Tier-III-Rechenzentren, einschließlich Sicherheit vor Ort rund um die Uhr, personell besetzte Zugangspunkte, Anti-Huckepack-Mechanismen, Zwei-Faktor-Authentifizierung und CCTV-Überwachung. Die von AWS, Azure oder Google Cloud genutzten Einrichtungen entsprechen den Standards für Tier-III-Rechenzentren.

M. ***Kontrolle des Zugangs zu den IT-Systemen***

Kontrollen des Datenverarbeiters

Der Datenverarbeiter kontrolliert wie folgt den Zugang zu den Systemen, auf denen die Serviceleistungen bereitgestellt werden:

1. Alle Mitarbeiter und Auftragnehmer des Datenverarbeiters erhalten eindeutige Benutzer-IDs. Die gemeinsame Nutzung eines Kontos ist nicht erlaubt.
2. Die Einhaltung der definierten Passwort-Vorgaben wird mit einem Passwort-Synchronisierungstool durchgesetzt. Die Vorgaben beinhalten:
    a. Mindestlänge von 12 Zeichen
    b. Darf nicht auf öffentlichen Listen mit verletzten Passwörtern erscheinen
    c. Die letzten 23 Passwörter dürfen nicht wiederverwendet werden
    d. Das Passwort muss alle 180 Tage geändert werden
    e. Kontosperrung nach fünf (5) fehlgeschlagenen Anmeldeversuchen
3. Der logische Zugang wird abhängig von der Funktion erteilt.
4. Im VPN zur Produktionsumgebung des Datenverarbeiters ist eine Audit-Protokollierung eingerichtet.
5. Die Überwachungsprotokolle werden von einem Tool zur Protokollaggregation und Alarmierung nahezu in Echtzeit überwacht. Die Warnmeldungen sind so konfiguriert, dass sie an die Gruppe „Globale Informationssicherheit“ des Datenverarbeiters gesendet werden.

N. ***Kontrolle des Zugangs zu Daten***

Die Kundendaten dürfen sich nicht in der Unternehmensumgebung des Auftragsverarbeiters befinden. Der Zugriff auf die Systeme, auf denen die Dienste gehostet werden, wird wie folgt kontrolliert:

1. Der Zugriff ist von der Funktion des Mitarbeiters beim Auftragsverarbeiter abhängig.

2. Der privilegierte Zugriff auf eine Produktionsumgebung des Auftragsverarbeiters ist dessen entsprechend berechtigten Mitarbeitern vorbehalten.

O. Im VPN und auf den Systemen in der Produktionsumgebung des Auftragsverarbeiters ist eine **Audit-Protokollierung** eingerichtet.

P. ***Implementierung von Zugangskontrollen auf Grundlage der „geringsten Rechte“***

Der Zugang zur Produktionsumgebung des Auftragsverarbeiters wird abhängig von der Funktion erteilt.

Q. ***Sicherheit während der Übertragung und Verarbeitung***

Der Auftragsverarbeiter darf nicht zulassen, dass Kundendaten in der Unternehmensumgebung des Auftragsverarbeiters gespeichert werden, in der sich dessen Mitarbeiter und Auftragnehmer befinden. Die Produktionsumgebung des Auftragsverarbeiters ist logisch und physisch von seiner Unternehmensumgebung getrennt:

1. Der Zugang zur Produktionsumgebung des Auftragsverarbeiters erfolgt über ein VPN mit Zwei-Faktor-Authentifizierung über vom Auftragsverarbeiter zugelassene Geräte und wird nur Mitarbeitern des Auftragsverarbeiters und Auftragnehmern gewährt, deren Rolle den Zugang erfordert.
2. Es sind Firewalls nach Industriestandard vorhanden, die so konfiguriert sind, dass Datenverkehr nur an den für die Ausführung der Dienste notwendigen Ports möglich ist und an allen anderen Ports standardmäßig nicht zugelassen wird.
3. Der gesamte Zugriff von Administratoren auf die gehosteten Weboberflächen der Dienste wird mit HTTPS/TLS verschlüsselt.

Systemzugriffskontrollen

1. LDAP wird für die Authentifizierung der Mitarbeiter des Auftragsverarbeiters an den Produktionsumgebungen verwendet.
2. Ein privilegierter Zugriff wird nur entsprechend berechtigten Mitarbeitern des Auftragsverarbeiters erteilt.

Endgeräte-Sicherheit

1. Die Endgeräte, die für den Zugriff auf die Produktionsumgebung des Datenverarbeiters verwendet werden, werden zentral verwaltet, verfügen über entsprechende Sicherheitspatches, führen standardisierte Sicherheitssoftware aus und werden regelmäßig auf Schwachstellen überprüft.

Serversicherheit

1. Sicherheitspatches werden je nach Wichtigkeit angewendet.
2. Unnötige Dienste sind deaktiviert.
3. Standardpasswörter werden geändert.

R. ***Sicherheit während der Datenübertragung über öffentliche Netzwerke***

1. Alle Administratorzugriffe durch den Auftragsverarbeiter auf die Dienste werden mit HTTPS/TLS verschlüsselt.

S. ***Kontrollen in der Implementierungs- und Betriebsphase***

Die von den Diensten bereitgestellten Funktionen werden automatisch ausgeführt und erfordern – außer für Analysezwecke und zur Behebung von Problemen mit den Diensten – kein menschliches Eingreifen. Die Dienste sind so ausgelegt, dass sie wie im Servicevertrag beschrieben funktionieren.

T. ***Rückverfolgbarkeit von Zugriffen, Änderungen und Löschungen***

Der Zugriff auf die von den Diensten genutzten Systeme wird wie folgt kontrolliert:

1. Der Zugriff wird auf der Grundlage der Rolle des Auftragsverarbeiters gewährt.

2. Der privilegierte Zugriff auf die Produktionsumgebung des Auftragsverarbeiters ist entsprechend berechtigten Mitarbeitern vorbehalten.
3. Im VPN und auf den Systemen in der Produktionsumgebung des Auftragsverarbeiters ist eine Audit-Protokollierung eingerichtet.
4. Von den Diensten erstellte Prüfprotokolle erfassen den Zugriff auf die Dienste durch Mitarbeiter des Datenverantwortlichen.

U. ***Sicherstellung einer konformen Datenverarbeitung***

Außer für Analysezwecke und zur Behebung von Problemen mit den Diensten verarbeiten die Mitarbeiter des Auftragsverarbeiters Kundendaten nicht manuell. Alle Kundendaten werden von den Diensten wie in der Dokumentation der Dienste beschrieben automatisch verarbeitet.

V. ***Sicherstellung der Verfügbarkeit***

Dies wird wie folgt erreicht:

1. Die Infrastruktur jeder Produktionseinrichtung ist im Hochverfügbarkeitsmodus konfiguriert, der unter anderem zwei Stromversorgungen und mindestens zwei unterschiedliche Netzwerkverbindungen umfasst.
2. Die Co-Location-Einrichtungen entsprechen den Tier-III-Standards für Rechenzentren, einschließlich redundanter Stromversorgung und redundanter Umweltkontrollen.
3. Die Co-Location-Einrichtungen verfügen über eigene Generatoren mit einem Kraftstoffvorrat für mindestens zwei (2) Tage.
4. Ein Maßnahmenplan für die Betriebskontinuität zum Schutz der Mitarbeiter des Datenverarbeiters und die Wiederherstellung von dessen Geschäftsprozessen wird dokumentiert und jährlich getestet.
5. Eine verteilte Überwachungsinfrastruktur überwacht die Verfügbarkeit und Leistung.
6. .

W. ***Datentrennung***

Die Dienste halten die Kundendaten getrennt. Dies wird wie folgt erreicht:

1. Die logische Trennung wird vom Dienst durch einige oder alle der folgenden Maßnahmen aufrechterhalten:
   a. Eindeutige Kunden-IDs für jeden Kunden, die zur Kennzeichnung von Kundendaten innerhalb des Dienstes verwendet werden;
   b. Eindeutige IPs; oder
   c. Eindeutige Verschlüsselungsschlüssel.

ANLAGE 2

Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates

STANDARDVERTRAGSKLAUSELN

Übermittlung von Verantwortlichen an Auftragsverarbeiter

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

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

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

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

(d) Der Anhang zu diesen Klauseln mit den darin enthaltenen Anlagen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

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

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

Klausel 3

Drittbegünstigte

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

(i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7

(ii) Klausel 8 – Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e

(iii) Klausel 9 – Klausel 9 Buchstaben a, c, d und e

(iv) Klausel 12 – Klausel 12 Buchstaben a, d und f

(v) Klausel 13

(vi) Klausel 15.1 Buchstaben c, d und e

(vii) Klausel 16 Buchstabe e

(viii) Klausel 18 – Klausel 18 Buchstaben 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 Anlage I.B aufgeführt.

Klausel 7 – fakultativ

Kopplungsklausel – nicht anwendbar

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.

Übermittlung von Verantwortlichen an Auftragsverarbeiter

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 Anlage I. B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3 **Transparenz**

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich des von den Parteien ausgefüllten Anhangs, unentgeltlich zur Verfügung. Soweit es zum Schutz von

Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anlage II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes des Anhangs zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt des Anhangs nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage 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 Anlage 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 Buchstabe 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 Buchstabe a im 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 beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „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 seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anlage 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 (im Folgenden „sensible Daten“), wendet der Datenimporteur die in Anlage 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 (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union (4) ansässig sind (im Folgenden „Weiterübermittlung“), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran 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; 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.

(4) Das Abkommen über den Europäischen Wirtschaftsraum (EWR-Abkommen) regelt die Einbeziehung der drei EWR-Staaten Island, Liechtenstein und Norwegen in den Binnenmarkt der Europäischen Union. Das Datenschutzrecht der Union, darunter die Verordnung (EU) 2016/679, ist in das EWR-Abkommen eingeschlossen und wurde in Anlage XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

Klausel 9

Einsatz von Unterauftragsverarbeitern

(a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG. Der Datenimporteur besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens [Zeitraum angeben] im Voraus ausdrücklich 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 Einwände 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 im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. (8) 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.

(8) Diese Anforderung ist gegebenenfalls vom Unterauftragsverarbeiter zu erfüllen, der diesen Klauseln gemäß Klausel 7 im Rahmen des betreffenden Moduls beitritt.

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 Anlage 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 Website 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 Absatz 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 für die Einhaltung der Verordnung (EU) 2016/679 durch den Datenexporteur in Bezug auf die Datenübermittlung zuständig ist, wie in Anlage I.C angegeben, handelt als zuständige Aufsichtsbehörde.
[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Verordnung (EU) 2016/679 gemäß deren Artikel 3 Absatz 2 fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 bestellt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Vertreter im Sinne von Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 niedergelassen ist (siehe Anlage I.C), handelt als zuständige Aufsichtsbehörde. [Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Verordnung (EU) 2016/679 gemäß deren Artikel 3 Absatz 2 fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 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 als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anlage I.C).

(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 und Gepflogenheiten, 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 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

(b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe a insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

(i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

(ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien (12);

(iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

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

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

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

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

---

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

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

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

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

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

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

15.2 **Überprüfung der Rechtmäßigkeit und Datenminimierung**

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

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

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

ABSCHNITT IV – SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

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

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

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

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

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

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

(d) 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. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

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

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies folgende Rechte beinhaltet: (a) das Recht des im Dienstleistungsvertrag angegebenen Landes, wenn der Dienstleistungsvertrag dem Recht eines EU-Mitgliedstaates unterliegt, oder (b) das Recht der Niederlande, wenn der Dienstleistungsvertrag dem Recht eines Drittlandes unterliegt.

Klausel 18
Gerichtsstand und Zuständigkeit

Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

(a) Die Parteien vereinbaren, dass dies (a) die im Dienstleistungsvertrag angegebenen Gerichte sind, wenn im Dienstleistungsvertrag ein Gericht eines EU-Mitgliedstaates bestimmt wurde, oder (b) die Gerichte von Amsterdam sind, wenn im Dienstleistungsvertrag ein Gericht eines Drittlandes bestimmt wurde.

(b) 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.

(c) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ERLÄUTERUNG:

ANHANG

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

ANLAGE I

A. **LISTE DER PARTEIEN**

Datenexporteur(e): Der Datenexporteur ist auf Seite 1 dieses Vertrags als der Verantwortliche angegeben.

Datenimporteur(e): Der Datenimporteur ist Proofpoint, Inc., ein Anbieter von Sicherheitsdienstleistungen für E-Mail und soziale Medien, Threat Analytics und Sicherheitsschulungen.

B. **BESCHREIBUNG DER DATENÜBERMITTLUNG**

Betroffene Personen sind die Mitarbeiter und Auftragnehmer des Verantwortlichen sowie die Mitarbeiter und Auftragnehmer von Kunden und Lieferanten des Verantwortlichen.

Datenkategorien: Die Datenkategorien sind in Anhang 1 dieses Vertrags angegeben. Der Verantwortliche übermittelt keine sensiblen Daten an Proofpoint.

Verarbeitungsvorgänge: Die Häufigkeit der Übermittlung, Art und Zweck der Verarbeitung und Speicherdauer sind in Anhang 1 dieses Vertrags angegeben.

C. **ZUSTÄNDIGE AUFSICHTSBEHÖRDE** ***Zuständigen Aufsichtsbehörde(n) gemäß Klausel 13 angeben***

[Wenn der Datenexporteur in einem EU-Mitgliedstaat niedergelassen ist:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Datenexporteur seinen eingetragenen Sitz hat.

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber in den territorialen Anwendungsbereich der Verordnung (EU) 2016/679 gemäß deren Artikel 3 Absatz 2 fällt und einen Vertreter gemäß Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt hat:] Die Aufsichtsbehörde des Mitgliedstaats, in dem der Datenexporteur seinen eingetragenen Sitz hat.

[Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den territorialen Anwendungsbereich dieser Verordnung fällt, ohne jedoch einen Vertreter gemäß Artikel 27 Absatz 2 der Verordnung (EU) 2016/679 benennen zu müssen:] Die Aufsichtsbehörde der Niederlande

ANLAGE II

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Die Sicherheits-, technischen und organisatorischen Maßnahmen sind in Anhang 2 dieses Vertrags dargelegt.

ANLAGE III

LISTE DER UNTERAUFTRAGSVERARBEITER

Die aktuelle Liste der Unterauftragsverarbeiter für die Serviceleistungen kann auf der Webseite zu Vertrauen von Proofpoint auf https://www.proofpoint.com/us/legal/trust eingesehen werden.