

Datenverarbeitungszusatz durch Bynder

Dieser Datenverarbeitungszusatz, einschließlich seiner Anhänge („DPA“), ergänzt die Vereinbarung zwischen dem Kunden und dem jeweiligen Bynder-Vertragspartner („Bynder“) bezüglich der Verwendung und des Zugriffs auf das Produkt („Vereinbarung“) und bildet einen integralen Bestandteil derselben, so wie dies in den Standard-Nutzungsbedingungen von Bynder (v.14) geregelt ist, die unter www.bynder.com/de/rechtliches/ („Bedingungen“) verfügbar sind. Der DPA enthält die Vereinbarung der Parteien in Bezug auf die Verarbeitung personenbezogener Daten des Kunden durch Bynder im Zusammenhang mit dem Produkt. Sofern in diesem DPA oder der Vereinbarung nicht anders definiert, haben alle im Abschnitt 1 dieses DPA aufgelisteten Begriffe die angegebenen Bedeutungen.

1. Definitionen

- „**AUFSICHTSBEHÖRDE**“ bezeichnet eine unabhängige Behörde, die von einem EU-Mitgliedstaat gemäß der DSGVO errichtet wird.
- „**AUFTRAGSVERARBEITER**“ bezeichnet das Unternehmen, das personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- „**BETROFFENE PERSON**“ bezeichnet die identifizierte oder identifizierbare Person, auf die sich personenbezogene Daten beziehen.
- „**DATENSCHUTZGESETZGEBUNG**“ bezeichnet alle Gesetze und Vorschriften, die auf die Verarbeitung personenbezogener Daten im Rahmen der Vereinbarung anwendbar sind.
- „**DSGVO**“ bezeichnet die Verordnung 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, unter Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
- „**EWR**“ bezeichnet den Europäischen Wirtschaftsraum.
- „**KUNDE**“ bezeichnet die juristische Person, die Vertragspartei der Vereinbarung mit Bynder ist.
- „**PERSONENBEZOGENE DATEN**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, sofern diese Daten von Bynder im Namen des Kunden verarbeitet werden.
- „**STANDARDSVERTRAGSKLAUSELN**“ bezeichnet Anhang 4, der diesem DPA gemäß dem Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 beigefügt ist und Teil des Europäischen Parlaments und des Rates bildet.
- „**UNTERAUFTRAGSVERARBEITER**“ bezeichnet einen von Bynder beauftragten Auftragsverarbeiter.
- „**VERANTWORTLICHER**“ bezeichnet das Unternehmen, das über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
- „**VERARBEITUNG**“ (und alle Zeitformen des dazugehörigen Verbs) bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

2. Verarbeitung personenbezogener Daten

- 2.1 Umfang, Rollen und Details der Verarbeitung. Dieser DPA, einschließlich aller Anhänge, gilt, wenn personenbezogene Daten von Bynder gemäß der Vereinbarung verarbeitet werden. In Bezug auf die Verarbeitung personenbezogener Daten ist der Kunde der Verantwortliche, Bynder der Auftragsverarbeiter, wobei Bynder Unterauftragsverarbeiter gemäß den in Abschnitt 6 unten dargelegten Anforderungen beauftragen kann. Die Dauer der Verarbeitung, die Art und der Zweck der Verarbeitung, die Arten personenbezogener Daten und Kategorien von Betroffenen, die im Rahmen dieses DPA verarbeitet werden, werden in Anhang 1 dieses DPA näher dargelegt.
- 2.2 Verarbeitung personenbezogener Daten durch den Kunden. Der Kunde ist verpflichtet, bei der Nutzung des Produkts personenbezogene Daten in Übereinstimmung mit den Anforderungen der Datenschutzgesetzgebung zu verarbeiten, einschließlich aller anwendbaren Anforderungen zur Benachrichtigung der betroffenen Personen über die Inanspruchnahme von Bynder als Auftragsverarbeiter. Um jeglichen Zweifel auszuschließen, sei festgehalten, dass die Weisungen des Kunden zur Verarbeitung personenbezogener Daten den Datenschutzgesetzen entsprechen müssen. Der Kunde trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit personenbezogener Daten und die Mittel, mit denen der Kunde in den Besitz personenbezogener Daten gekommen ist.
- 2.3 Verarbeitung personenbezogener Daten durch Bynder. Bynder ist verpflichtet, personenbezogene Daten als vertrauliche Informationen zu behandeln und personenbezogene Daten im Namen des Kunden und nur in Übereinstimmung mit den dokumentierten Weisungen des Kunden für folgende Zwecke zu verarbeiten: (i) Verarbeitung in Übereinstimmung mit der Vereinbarung und den anwendbaren Bestellformularen; und (ii) Verarbeitung, die von Benutzern bei ihrer Nutzung des Produkts veranlasst wird.

3. Weisungen

- 3.1 Verbundene Unternehmen des Kunden. Der Kunde erklärt hiermit, dass er befugt ist, Bynder Weisungen bezüglich der Datenverarbeitung von personenbezogenen Daten zu erteilen und anderweitig im Namen von verbundenen Unternehmen des Kunden im Rahmen dieses DPA zu handeln.
- 3.2 Dokumentierte Anweisungen. Dieser DPA und die Vereinbarung sind die vollständigen und endgültigen dokumentierten Weisungen des Kunden zum Zeitpunkt der Unterzeichnung der Vereinbarung mit Bynder über die Verarbeitung personenbezogener Daten. Zusätzliche oder alternative Weisungen sind gesondert und schriftlich zu vereinbaren.
- 3.3 Ausnahme. Wenn Bynder gesetzlich verpflichtet ist, eine zusätzliche Verarbeitungstätigkeit durchzuführen, wird Bynder den Kunden vor Beginn dieser Verarbeitungstätigkeit über diese gesetzliche Anforderung informieren, es sei denn, eine solche Mitteilung ist gesetzlich verboten.

3.4 Weisungen, die gegen die Datenschutzgesetzgebung verstoßen könnten. Wenn eine Weisungen des Kunden nach Ansicht von Bynder gegen die Datenschutzgesetzgebung verstoßen könnten, ist Bynder berechtigt, die Befolgung dieser Weisungen abzulehnen und wird den Kunden über die Gründe für die Ablehnung informieren. In solchen Fällen muss der Kunde rechtzeitig alternative Weisungen erteilen und Bynder kann die Verarbeitung der betroffenen personenbezogenen Daten (mit Ausnahme ihrer sicheren Speicherung) so lange aussetzen, bis Bynder annehmbare Weisungen erhält.

4. Personal von Bynder

4.1 Geheimhaltungspflichten. Bynder wird dafür Sorge tragen, dass sein Personal, das mit der Verarbeitung personenbezogener Daten befasst ist, über den vertraulichen Charakter der personenbezogenen Daten informiert wird und schriftliche Vertraulichkeitsvereinbarungen unterzeichnet hat.

4.2 Begrenzter Zugriff. Bynder wird dafür Sorge tragen, dass der Zugriff von Bynder auf personenbezogene Daten auf jenes Personal beschränkt ist, das Dienstleistungen in Übereinstimmung mit der Vereinbarung erbringt.

4.3 Datenschutzbeauftragter. Bynder hat einen Datenschutzbeauftragten („DPO“) bestellt. Der bestellte DPO ist unter privacy@bynder.com erreichbar.

5. Sicherheit der Verarbeitung

5.1 Maßnahmen. Bynder hat geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, oder unbefugten Offenlegung und Zugriff („Sicherheitsmaßnahmen“) ergriffen und wird diese beibehalten, so wie in Anhang 3 dieses DPA beschrieben, einschließlich gegebenenfalls:

- der Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- der Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Datenverarbeitungssystemen zu gewährleisten;
- vorbehaltlich des Service Level Agreements die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugriff zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; und
- der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

5.2 Der Kunde hat eigenständig beurteilt, ob die Sicherheitsmaßnahmen, so wie in Anhang 3 dieses DPA beschrieben, den Anforderungen des Kunden entsprechen.

5.3 Zertifizierungen Dritter. Bynder hat Zertifizierungen Dritter gemäß Anhang 3 dieses DPA erhalten. Auf schriftliches Verlangen des Kunden, jedoch nicht mehr als einmal pro Jahr und vorbehaltlich der in der Vereinbarung festgelegten Geheimhaltungsverpflichtungen, stellt Bynder dem Kunden eine Kopie der jeweils neuesten Drittzertifizierung und des Auditberichts von Bynder, soweit zutreffend, zur Verfügung.

6. Unterauftragsverarbeiter

6.1 Allgemeine Genehmigung. Der Kunde stimmt zu, dass Bynder Unterauftragsverarbeiter beauftragen kann, um Bynders vertragliche Verpflichtungen aus diesem DPA zu erfüllen oder bestimmte Dienstleistungen in Bynders Namen zu erbringen.

6.2 Pflichten des Unterauftragsverarbeiters. Bynder wird eine schriftliche Vereinbarung mit dem Unterauftragsverarbeiter schließen und Bynder wird, soweit der Unterauftragsverarbeiter die gleichen Verarbeitungsaktivitäten durchführt, die von Bynder bereitgestellt werden, dem Unterauftragsverarbeiter Datenschutzverpflichtungen auferlegen, die den Anforderungen dieses DPA entsprechen.

6.3 Liste der Unterauftragsverarbeiter. Bynder beauftragt derzeit die in Anhang 2 dieses DPA aufgeführten Unterauftragsverarbeiter. Eine Liste der Unterauftragsverarbeiter ist auch auf der Website von Bynder unter www.bynder.com/de/rechtliches/unterauftragsverarbeiter („Seite der Unterauftragsverarbeiter“) zu finden. Bynder aktualisiert die Seite der Unterauftragsverarbeiter mit allen Änderungen durch Hinzuziehung oder Ersetzen von Unterauftragsverarbeiter und unterrichtet den Kunden mindestens sieben Kalendertage im Voraus, bevor diese Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten beginnen.

6.4 Widerspruchsrecht. Der Kunde kann der Einsetzung eines neuen Unterauftragsverarbeiters auf angemessener und legitimer Grundlage widersprechen. Für den Fall, dass sich der Kunde gegen einen neuen Unterauftragsverarbeiter ausspricht, muss der Kunde innerhalb der in Abschnitt 6.3 festgelegten Frist von sieben Kalendertagen eine schriftliche Mitteilung an privacy@bynder.com senden, in der die spezifischen Bedenken des Kunden bezüglich des neuen Unterauftragsverarbeiters dargelegt sind, um Bynder so die Möglichkeit zu geben, auf diese Bedenken zu reagieren. Bynder kann nach eigenem Ermessen (i) den Unterauftragsverarbeiter nicht ernennen und/oder einen alternativen Unterauftragsverarbeiter vorschlagen; (ii) Schritte unternehmen, um die spezifischen Bedenken des Kunden zu berücksichtigen; oder (iii) dem Kunden das Bynder-Produkt ohne jenen besonderen Aspekt zur Verfügung stellen, der die Einsetzung des beanstandeten Unterauftragsverarbeiters beinhalten würde. Wenn Bynder nicht in der Lage ist oder nach vernünftigem Ermessen feststellt, dass es wirtschaftlich unvernünftig ist, eine der Optionen in Abschnitt 6.4 (i)-(iii) zu erfüllen, kann der Kunde die Vereinbarung gemäß Abschnitt 19.3 der Bedingungen kündigen.

6.5 Haftung. Bynder bleibt für die Leistung eines Unterauftragsverarbeiters in demselben Umfang verantwortlich, in dem Bynder verantwortlich wäre, wenn es die Leistungen des jeweiligen Unterauftragsverarbeiters gemäß den Bedingungen dieses DPA direkt ausführen würde.

7. Rechte einer betroffenen Person

Bynder wird, soweit gesetzlich zulässig, den Kunden unverzüglich benachrichtigen, wenn Bynder eine Anfrage einer betroffenen Person hinsichtlich der Ausübung der Rechte der betroffenen Person gemäß der Datenschutzgesetzgebung, insbesondere Kapitel III der DSGVO, erhält („Anfrage der betroffenen Person“). Unter Berücksichtigung der Art der Verarbeitung wird Bynder den Kunden durch geeignete technische und organisatorische Maßnahmen unterstützen, soweit dies möglich ist, damit der Kunde seiner Verpflichtung zur Beantwortung von Anfragen betroffener Personen im Rahmen der Datenschutzgesetzgebung nachkommen kann.

Soweit der Kunde eine Anfrage der betroffenen Person nicht bearbeiten kann, wird Bynder auf Anfrage des Kunden wirtschaftlich angemessene Anstrengungen unternehmen, um den Kunden bei der Beantwortung dieser Anfrage der betroffenen Person zu unterstützen. Soweit gesetzlich zulässig, ist der Kunde für alle Kosten verantwortlich, die sich aus der Bereitstellung einer solchen Unterstützung durch Bynder ergeben.

8. Unterstützung des Kunden bei der Erfüllung eigener Pflichten

Unter Berücksichtigung der Art der Verarbeitung und der Bynder zur Verfügung stehenden Informationen unterstützt Bynder den Kunden in angemessener Weise bei der Erfüllung seiner einschlägigen Verpflichtungen gemäß Artikel 32 bis 36 DSGVO. Soweit gesetzlich zulässig, ist der Kunde für alle Kosten verantwortlich, die sich aus der Bereitstellung einer solchen Unterstützung durch Bynder ergeben.

9. Meldung von Verletzungen des Schutzes personenbezogener Daten

Bynder benachrichtigt den Kunden unverzüglich, jedenfalls stets innerhalb von 48 Stunden, nachdem Bynder von der unbeabsichtigten oder unrechtmäßigen Vernichtung, dem Verlust, der Veränderung, der unbefugten Offenlegung oder dem Zugriff auf personenbezogene Daten, die von Bynder oder seinen Unterauftragsverarbeitern übermittelt, gespeichert oder anderweitig verarbeitet wurden, Kenntnis erlangt hat („Verstöße beim Schutz personenbezogener Daten“). Die Benachrichtigung über Verstöße beim Schutz personenbezogener Daten, falls zutreffend, wird per E-Mail an die E-Mail-Adresse gesendet, die für Mitteilungen im entsprechenden Bestellformular angegeben ist; falls keine E-Mail-Adresse angegeben ist, erfolgt die Mitteilung an einen oder mehrere Produktadministrator(en) des Kunden. Bynders Verpflichtung, den Kunden über eine Verletzung des Schutzes personenbezogener Daten zu informieren, stellt keine Anerkennung eines Verschuldens oder einer Haftung durch Bynder in Bezug auf die Verletzung des Schutzes personenbezogener Daten dar. Die Verpflichtungen aus diesem Abschnitt 9 gelten nicht für Vorfälle, die vom Kunden oder seinen Benutzern verursacht werden.

10. Rückgabe und Löschung personenbezogener Daten

- 10.1 Auf Verlangen des Kunden in Form einer Mitteilung an privacy@bynder.com wird Bynder personenbezogene Daten in Übereinstimmung mit den in der Vereinbarung festgelegten Zeiträumen zurückgeben oder löschen, es sei denn, EU-Recht oder die Gesetze eines EU-Mitgliedstaats verlangen, dass Bynder die personenbezogenen Daten aufbewahrt. Bynder wird personenbezogene Daten 180 Kalendertage nach Beendigung oder Ablauf der Vereinbarung löschen. Bynder ist verpflichtet, personenbezogene Daten in Übereinstimmung mit der/den neuesten Methode(n) zur Datenbereinigung zu entsorgen, so wie in NIST 800-88 („Richtlinien für die Medienbereinigung“) beschrieben.
- 10.2 Ungeachtet gegenteiliger Bestimmungen in diesem DPA kann Bynder personenbezogene Daten aufbewahren, wenn und solange dies gesetzlich vorgeschrieben ist.
- 10.3 Personenbezogene Daten, die in den automatischen Backup- oder Archivierungssystemen von Bynder gespeichert sind, werden automatisch 180 Tage nach dem Backup oder ansonsten so schnell wie technisch möglich gelöscht.
- 10.4 Wenn der Kunde personenbezogene Daten auf einer Festplatte oder anderen Formen von Wechselmedien bereitstellt, müssen diese Wechselmedien verschlüsselt oder passwortgeschützt sein. Bynder wird in Zusammenarbeit mit dem Kunden entweder die Wechselmedien an den Kunden zurückgeben oder diese Wechselmedien durch einen zertifizierten Dritten sicher vernichten. Ein Vernichtungszertifikat kann dem Kunden auf Anfrage zur Verfügung gestellt werden.

11. Kontrollrechte des Kunden

- 11.1 Zusammenfassender Bericht der Internen Revision. Zusätzlich zu Abschnitt 5.3 prüft Bynder regelmäßig die Sicherheit der Datenverarbeitungssysteme. Auf schriftliches Verlangen des Kunden wird Bynder dem Kunden eine Zusammenfassung der Ergebnisse dieser Prüfung („Zusammenfassender Bericht“) zur Verfügung stellen, um die Einhaltung der Verpflichtungen aus diesem DPA nachzuweisen.
- 11.2 Kontrolle durch den Kunden. Wenn der Kunde belegt, dass der zusammenfassende Bericht die Einhaltung dieses DPA von Bynder nicht zufriedenstellend nachweisen kann und dass er einen begründeten Verdacht hegt, dass Bynder gegen diesen DPA verstößt, kann der Kunde eine Kontrolle in den Räumlichkeiten von Bynder, jedoch nicht öfter als einmal pro Jahr und vorbehaltlich der in der Vereinbarung festgelegten Geheimhaltungsverpflichtungen und der folgenden Bedingungen, durchführen:
- Der Kunde muss mindestens 30 Tage im Voraus eine schriftliche Mitteilung an privacy@bynder.com senden. Eine solche Mitteilung muss die Gründe für den Kontrollantrag angeben und wird mit der Eingangsbestätigung von Bynder wirksam.
 - Kontrollen werden innerhalb eines einvernehmlich vereinbarten Umfangs, einer einvernehmlich bestimmten Dauer und eines einvernehmlich festgelegten Zeitplans durchgeführt; sie werden vom Kunden oder einem von Bynder vorab genehmigten Dritten durchgeführt, wobei diese Genehmigung nicht unangemessen verweigert werden darf; und die Kontrollen werden innerhalb der normalen Geschäftszeiten von Bynder und nach besten Kräften so durchgeführt, dass Störungen des Geschäftsbetriebs von Bynder vermieden werden.
- 11.3 Kosten. Die Kosten einer Kontrolle in den Räumlichkeiten von Bynder gemäß Abschnitt 11.2 gehen zu Lasten des Kunden, es sei denn, es wird ein wesentlicher Verstoß (so wie in der Vereinbarung definiert) gegen diesen DPA festgestellt. In diesem Fall trägt Bynder die Kosten.
- 11.4 Nichts in diesem Abschnitt 11 ändert oder modifiziert die Standardvertragsklauseln oder beeinträchtigt die Rechte einer Aufsichtsbehörde oder einer betroffenen Person gemäß den Standardvertragsklauseln.

12. Internationale Datenübermittlung

- 12.1 Regionen. Der Kunde kann den Ort, an dem die Kundendaten, einschließlich personenbezogener Daten, gehostet werden, in der Vereinbarung angeben („Region“). Sofern nicht anders in diesem DPA vereinbart, oder zur Bereitstellung des vom Kunden in Auftrag gegebenen Produkts und der vom Kunden in Auftrag gegebenen Dienstleistungen oder zur Einhaltung gesetzlicher Bestimmungen

erforderlich ist, wird Bynder keine personenbezogenen Daten aus der vom Kunden ausgewählten Region übermitteln. Eine Überführung in ein Drittland findet nur statt, wenn die Bedingungen des Kapitels V der DSGVO erfüllt sind.

12.2 Anwendung von Standardvertragsklauseln. Bynder schließt Standardvertragsklauseln mit jedem verbundenen Unternehmen und/oder Unterauftragsverarbeiter ab, wenn die Verarbeitung personenbezogener Daten außerhalb des EWR in ein Drittland übertragen wird, das von der Europäischen Kommission nicht als ein Land anerkannt wird, das ein angemessenes Schutzniveau für personenbezogene Daten bietet. Der Kunde ermächtigt Bynder hiermit, Standardvertragsklauseln (auch) in seinem Namen abzuschließen und beauftragt Bynder, diese gegebenenfalls im Namen des Kunden gegen den jeweiligen Unterauftragsverarbeiter durchzusetzen. Die Standardvertragsklauseln gelten nicht für personenbezogene Daten, die nicht außerhalb des EWR übertragen werden.

12.3 Rangfolge. Wenn die Standardvertragsklauseln gelten, ändert oder modifiziert nichts in diesem Abschnitt 12 die Standardvertragsklauseln.

13. Haftungsbeschränkung

Die Gesamthaftung jeder Partei, die sich aus diesem DPA ergibt oder mit ihm zusammenhängt, ob aus Vertrag, unerlaubter Handlung oder einer anderen Haftungstheorie, unterliegt dem Abschnitt „Haftungsbeschränkung“ der Vereinbarung, und jede Bezugnahme in diesem Abschnitt auf die Haftung einer Partei steht für die Gesamthaftung dieser Partei und aller ihrer verbundenen Unternehmen im Rahmen der Vereinbarung und aller DPAs zusammen.

14. Gesamte Vereinbarung, Hierarchie

Mit Ausnahme der Änderungen, die durch diesen DPA vorgenommen werden, bleibt die Vereinbarung in vollem Umfang in Kraft und wirksam. Wenn es einen Konflikt zwischen einer anderen Vereinbarung zwischen den Parteien, einschließlich der Vereinbarung und diesem DPA, gibt, haben die Bedingungen dieses DPA im Umfang des Konflikts Vorrang.

15. Laufzeit und Kündigung

Dieser DPA tritt gleichzeitig mit der Vereinbarung in Kraft und endet automatisch bei Beendigung oder Ablauf der Vereinbarung.

16. Liste der Anhänge

Anhang 1: Details der Verarbeitung personenbezogener Daten
Anhang 2: Liste der Unterauftragsverarbeiter und Bynder-Unternehmen
Anhang 3: Sicherheitsmaßnahmen
Anhang 4: Standardvertragsklauseln

17. Übersetzungen

Die deutsche Version dieses DPA wird lediglich aus Gründen der Kundenannehmlichkeit zur Verfügung gestellt. Sollte eine Mehrdeutigkeit oder ein Konflikt zwischen verschiedenen Übersetzungen bestehen, so ist die englische Fassung maßgeblich und ausschlaggebend.

Anhang 1: Details der Verarbeitung personenbezogener Daten

Art und Zweck der Verarbeitung

Bynder wird personenbezogene Daten verarbeiten, soweit dies zur Bereitstellung des Produkts gemäß der Vereinbarung und gemäß weiteren Weisungen des Kunden bei seiner Nutzung des Produkts erforderlich ist.

Dauer der Verarbeitung

Vorbehaltlich des Abschnitts 10 dieses DPA wird Bynder personenbezogene Daten für die Dauer der Vereinbarung verarbeiten, sofern nichts anderes schriftlich vereinbart wurde.

Kategorien betroffener Personen

Der Kunde kann personenbezogene Daten im Produkt speichern, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird. Die einzigen personenbezogenen Daten, die für die Nutzung des Produkts erforderlich sind, beziehen sich auf folgende Kategorien betroffener Personen:

- Mitarbeiter des Kunden
- Benutzer des Kunden

Arten personenbezogener Daten

Der Kunde kann personenbezogene Daten im Produkt speichern, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird. Die einzigen Arten personenbezogener Daten, die für die Nutzung des Produkts erforderlich sind, sind:

- Vor- und Nachname
- E-Mail-Adresse

Besondere Arten von personenbezogenen Daten

Der Kunde darf keine besonderen Arten von personenbezogenen Daten im Produkt speichern. Das Produkt ist nicht dafür bestimmt besondere Arten von personenbezogenen Daten des Kunden zu speichern. Dabei geht es um personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten.

Anhang 2: Unterauftragsverarbeiter und Bynder-Unternehmen

Infrastrukturanbieter

Bynder beauftragt folgende(n) Unterauftragsverarbeiter, um Kundendaten zu hosten und zu speichern.

Name des Unternehmens	Tätigkeit des Unterauftragsverarbeiters	Land des Unternehmens
Amazon Web Services EMEA SARL	Anbieter von Cloud-Diensten	Luxemburg
Google Ireland, Inc.	Anbieter von Cloud-Diensten (nur für Video Brand Studio)	Irland

Sonstige Unterauftragsverarbeiter

Bynder arbeitet mit bestimmten Dritten zusammen, so wie unten aufgeführt, um spezifische Funktionalitäten innerhalb des Produkts bereitzustellen. Um die entsprechende Funktionalität bereitzustellen, greifen diese Unterauftragsverarbeiter auf Kundendaten zu. Ihre Verwendung beschränkt sich auf die angegebenen Aktivitäten:

Name des Unternehmens	Tätigkeit des Unterauftragsverarbeiters	Land des Unternehmens
Pricon BV	Pricon ist ein Callcenter, das Bynder bei der Bereitstellung von Telefonsupport außerhalb der Bürozeiten unterstützt.	Niederlande
Zendesk Inc.	Zendesk bietet ein Cloud-basiertes System zur Verfolgung und Lösung von Kundensupport-Tickets.	Vereinigte Staaten
Drift.com Inc.	Drift ermöglicht eine direkte Kommunikation mit dem Kunden innerhalb des Produkts.	Vereinigte Staaten
Appcues, Inc.	Appcues ermöglicht Bynder, In-App-Benachrichtigungen bereitzustellen.	Vereinigte Staaten.

Bynder beauftragt außerdem folgende Unterauftragsverarbeiter mit dem Support für das Video Brand Studio-Modul.

Name des Unternehmens	Tätigkeit des Unterauftragsverarbeiters	Land des Unternehmens
Google Ireland, Inc.	Google stellt zudem ein Leistungs- und Diagnosetool zur Verfügung, mit dem der Zustand der Google-Ressourcen und -Anwendungen überwacht und gemessen werden kann.	Irland
FileStack, Inc.	FileStack unterstützt das Hochladen von Kundendaten im Video Brand Studio-Modul.	Vereinigte Staaten

Bynder-Unternehmen

Die folgenden Unternehmen sind Teil der Unternehmensstruktur von Bynder. Je nach geografischem Standort des Kunden kann Bynder auch eines oder mehrere der folgenden Unternehmen als Unterauftragsverarbeiter beauftragen.

Name des Unternehmens	Art des Unternehmens	Land des Unternehmens
Bynder B.V.	Muttergesellschaft	Niederlande
Bynder LLC	Tochtergesellschaft	Vereinigte Staaten
Bynder Ltd.	Tochtergesellschaft	Vereinigtes Königreich
Bynder Software FZ-LLC	Tochtergesellschaft	Dubai
Bynder Software SL	Tochtergesellschaft	Spanien

Content Deliver Networks („CDN“)

Bynder kann ein CDN einsetzen, um die Lieferung des Produkts zu unterstützen. CDNs haben selbst keinen Zugriff auf Kundendaten, sondern sind Systeme, die üblicherweise für die schnelle Bereitstellung von Inhalten auf der Grundlage des geografischen Standorts einer Person, die auf die Inhalte zugreift, und der Herkunft des Inhaltsanbieters verwendet werden:

CDN-Anbieter	CDN-Standort
Amazon Web Services EMEA SARL	Weltweit

Anhang 3: Sicherheitsmaßnahmen

Bynder wird folgende Sicherheitsmaßnahme ergreifen und aufrechterhalten, um die personenbezogenen Daten des Kunden angemessen zu schützen. Der Kunde versteht und stimmt zu, dass diese Sicherheitsmaßnahmen dem technischen Fortschritt und der Entwicklung unterliegen und Bynder daher ausdrücklich gestattet ist, angemessene alternative Maßnahmen umzusetzen, solange das in diesem Anhang 3 beschriebene allgemeine Sicherheitsniveau aufrechterhalten wird:

1. Technische Maßnahmen

- 1.1. Zugriffskontrolle. Bynder muss unbefugten Zugriff auf Datenverarbeitungssysteme verhindern. Mitarbeiter haben nur dann Zugriff auf Kundendaten, wenn dies für die Erfüllung ihrer Aufgaben erforderlich ist. Kundendaten dürfen nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden.
- 1.2. Zutrittskontrolle. Bynder muss verhindern, dass Unbefugte auf Datenverarbeitungssysteme zugreifen können.
- 1.3. Logging-Kontrolle. Bynder muss sicherstellen, dass alle Ereignisse in den Datenverarbeitungssystemen nachträglich überprüft werden können.
- 1.4. Übertragungskontrolle. Bynder muss dafür Sorge tragen, dass personenbezogene Daten während der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- 1.5. Daten im Ruhezustand. Bynder muss für eine angemessene Verschlüsselung der Daten im Ruhezustand sorgen.
- 1.6. Trennungskontrolle. Bynder muss sicherstellen, dass für verschiedene Zwecke erhobene Daten getrennt verarbeitet werden.
- 1.7. Zuverlässigkeitskontrolle. Bynder muss dafür sorgen, dass alle Funktionen des Datenverarbeitungssystems verfügbar sind und auftretende Störungen gemeldet werden.
- 1.8. Integritätskontrolle. Bynder muss sicherstellen, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können oder dass beschädigte Daten durch die ursprünglichen und richtigen Daten ersetzt werden können.
- 1.9. Verfügbarkeitskontrolle. Bynder muss sicherstellen, dass personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt und daher für den Kunden verfügbar sind.

2. Organisatorische Maßnahmen

- 2.1 Zugangskontrolle. Bynder muss verhindern, dass sich Unbefugte Zugang zu den Räumlichkeiten von Bynder verschaffen.
- 2.2 Sicherheits- und Sensibilisierungsschulungen. Bynder muss ein Programm zur Förderung des Sicherheitsbewusstseins unterhalten, das eine entsprechende Schulung des Personals zu den Sicherheitsrichtlinien von Bynder umfasst.
- 2.3 Personalprüfung. Für alle Mitarbeiter sind vor der Einstellung strafrechtliche Hintergrundprüfungen durchzuführen. Darüber hinaus muss Bynder dafür Sorge tragen, dass alle Mitarbeiter schriftliche Vertraulichkeitsvereinbarungen abgeschlossen haben.
- 2.4 Managementprozess der Informationssicherheit. Bynder unterhält ein nach ISO 27001:2013 zertifiziertes Informationssicherheitsmanagementsystem.
- 2.5 Prozess des Betriebskontinuitäts-Managements. Bynder unterhält ein Betriebskontinuitäts-Management-System, das die Prozesse und Verfahren für den Katastrophenfall definiert, einschließlich der Prüfung und Überprüfung der Notfallpläne.
- 2.6 Regelmäßige Evaluierung der Sicherheitsmaßnahmen. Bynder stellt ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen sicher, um ein dem Risiko der Verarbeitung angemessenes Sicherheitsniveau zu gewährleisten.

3. Zertifizierungen Dritter

Bynder besitzt und hält derzeit folgende Zertifizierungen aufrecht:

- ISO 27001:2013
- ISO 27018:2019
- ISO 22301:2019

Anhang 4: Standardvertragsklauseln

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/914 DER KOMMISSION 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)¹ bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.
- b) Die Parteien:
- i) die in Anhang I.A aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und
 - ii) die in Anhang I.A aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“),

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

- c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang I.B.
- d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

- a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 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 in der Anlage. 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:

¹ Handelt es sich bei dem Datenexporteur um einen Auftragsverarbeiter, der der Verordnung (EU) 2016/679 unterliegt und der im Auftrag eines Organs oder einer Einrichtung der Union als Verantwortlicher handelt, so gewährleistet der Rückgriff auf diese Klauseln bei der Beauftragung eines anderen Auftragsverarbeiters (Unterauftragsverarbeitung), der nicht unter die Verordnung (EU) 2016/679 fällt, ebenfalls die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39), insofern als diese Klauseln und die gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegten Datenschutzpflichten angeglichen sind. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die im Beschluss 2021/915 enthaltenen Standardvertragsklauseln stützen.

- i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7
 - ii) Klausel 8 — Modul eins: Klausel 8.5 Buchstabe e und Klausel 8.9 Buchstabe b Modul zwei: Klausel 8.1 Buchstabe b, Klausel 8.9 Buchstaben a, c, d und e Modul drei: Klausel 8.1 Buchstaben a, c und d und Klausel 8.9 Buchstaben a, c, d, e, f und g Modul vier: Klausel 8.1 Buchstabe b und Klausel 8.3 Buchstabe b
 - iii) Klausel 9 — Modul zwei: Klausel 9 Buchstaben a, c, d und e Modul drei: Klausel 9 Buchstaben a, c, d und e
 - iv) Klausel 12 — Modul eins: Klausel 12 Buchstaben a und d Module zwei und drei: 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 — Module eins, zwei und drei Klausel 18 Buchstaben a und b Modul vier: Klausel 18
- 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 Anhang I.B aufgeführt.

Klausel 7 — fakultativ

Nicht gebraucht

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

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

8.1. Weisungen

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

8.2. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang 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 der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang II beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf 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 Anhang 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 seiner Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang 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 personenbezogener 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 Anhang 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 Union² 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.

² 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 einbezogen und wurde in Anhang XI aufgenommen. Daher gilt eine Weitergabe durch den Datenimporteur an einen im EWR ansässigen Dritten nicht als Weiterübermittlung im Sinne dieser Klauseln.

- 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.

Klausel 9

Einsatz von Unterauftragsverarbeitern

- a) Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens sieben Tage 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.³ Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.
- c) Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- d) Der Datenimporteur haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Datenimporteur geschlossenen Vertrag nachkommt. Der Datenimporteur benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.
- e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 10

Rechte betroffener Personen

- a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.
- b) Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in

³ Diese Anforderung ist gegebenenfalls vom Unterauftragsverarbeiter zu erfüllen, der diesen Klauseln gemäß Klausel 7 im Rahmen des betreffenden Moduls beiträgt.

Anhang 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 dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).

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

Wenn der Datenexporteur nicht in einem EU-Mitgliedstaat niedergelassen ist, aber nach Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 in den räumlichen Anwendungsbereich dieser Verordnung 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 Anhang 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,⁴
 - 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.

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

⁴ 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.

- 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 das Recht welches in der Vereinbarung festgelegt ist, sofern dies das Recht eines der EU-Mitgliedstaaten ist, das Rechte Drittbegünstigte zulässt, andernfalls gilt das Recht der Niederlande ist.

Klausel 18

Gerichtsstand und Zuständigkeit

- a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.
- b) Die Parteien vereinbaren, dass dies die Gerichte von eines der EU-Mitgliedstaaten ist, wie in Klausel 17 ausgelegt sind.
- c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.
- d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANLAGE

ANHANG I

A. LISTE DER PARTEIEN

Datenexporteur(e):

1. Name: Die Vertragspartei welche als **Kunde** in der DPA definiert ist.

Anschrift: die Adresse spezifiziert/hinterlegt in der DPA oder im Vereinbarung.

Name, Funktion und Kontaktdaten der Kontaktperson: die Kontaktdaten spezifiziert/hinterlegt in der DPA oder im Vereinbarung.

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Nutzung der Bynder Produktes / der Bynder Produkte.

Unterschrift und Datum: Durch den Abschluss der Vereinbarung wird davon ausgegangen, dass der Datenexporteur diese Standardvertragsklauseln einschließlich ihrer Anhänge zum Datum des Inkrafttretens der Vereinbarung unterzeichnet hat.

Rolle (Verantwortlicher/Auftragsverarbeiter): Verantwortlicher

Datenimporteur(e):

1. Name: **Bynder LLC**

Anschrift: 321 Summer Street, Boston MA 02210, USA.

Name, Funktion und Kontaktdaten der Kontaktperson: die Kontaktdaten spezifiziert/hinterlegt in der DPA oder im Vereinbarung.

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: Bereitstellung des Bynder Produktes /der Bynder Produkte.

Unterschrift und Datum: Durch den Abschluss der Vereinbarung wird davon ausgegangen, dass der Datenimporteur diese Standardvertragsklauseln einschließlich ihrer Anhänge zum Datum des Inkrafttretens der Vereinbarung unterzeichnet hat.

Rolle (Verantwortlicher/Auftragsverarbeiter): Auftragsverarbeiter

B. BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

Der Kunde kann personenbezogene Daten im Produkt speichern, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird. Die einzigen personenbezogenen Daten, die für die Nutzung des Produkts erforderlich sind, beziehen sich auf folgende Kategorien betroffener Personen:

- Mitarbeiter des Kunden
- Benutzer des Kunden

Kategorien der übermittelten personenbezogenen Daten

Der Kunde kann personenbezogene Daten im Produkt speichern, deren Umfang vom Kunden nach eigenem Ermessen bestimmt und kontrolliert wird. Die einzigen Arten personenbezogener Daten, die für die Nutzung des Produkts erforderlich sind, sind:

- Vor- und Nachname
- E-Mail-Adresse

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

Der Kunde darf keine besonderen Arten von sensiblen Daten im Produkt speichern. Das Produkt ist nicht dafür bestimmt sensible Daten des Kunden zu speichern. Dabei geht es um personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten.

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

Die Häufigkeit der Übertragung ist für die Dauer der Vereinbarung fortlaufend, sofern nicht schriftlich anderweitig vereinbar.

Art der Verarbeitung

Bynder wird personenbezogene Daten verarbeiten, soweit dies zur Bereitstellung des Produkts gemäß der Vereinbarung und gemäß weiteren Weisungen des Kunden bei seiner Nutzung des Produkts erforderlich ist.

Zweck(e) der Datenübermittlung und Weiterverarbeitung

Bynder wird personenbezogene Daten verarbeiten, soweit dies zur Bereitstellung des Produkts gemäß der Vereinbarung und gemäß weiteren Weisungen des Kunden bei seiner Nutzung des Produkts erforderlich ist.

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

Bynder kann personenbezogene Daten sechs Monate nach Beendigung oder Ablauf der Vereinbarung löschen, es sei denn, das Recht der Europäischen Union oder die Gesetze eines EU-Mitgliedstaats verlangen, dass Bynder die personenbezogenen Daten für einen längeren Zeitraum speichert. Personenbezogene Daten, die in Bynders Auto-Backup- oder Archivierungssystemen gespeichert sind, werden automatisch nach 180 Tagen nach der Sicherung oder so schnell wie technisch möglich gelöscht.

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

Spezifiziert auf der Bynder-Website unter www.bynder.com/sub-processors/ („Sub-Processors-Seite“). Unterauftragsverarbeiter verarbeiten personenbezogene Daten für die Dauer der Vereinbarung, sofern nicht schriftlich anderes vereinbart.

C. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

Die zuständige Aufsichtsbehörde des Datenexporteurs wird nach der DSGVO ermittelt.

ANHANG II

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

Beschreibung der von dem/den Datenimporteur(en) ergriffenen technischen und organisatorischen Maßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen

Der Datenimporteur wird technischen und organisatorischen Maßnahmen ergreifen und aufrechterhalten, um die personenbezogenen Daten des Datenexporteurs angemessen zu schützen, wie im DPA näher beschrieben. Der Datenexporteur nimmt zur Kenntnis und stimmt zu, dass diese technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen und Bynder daher ausdrücklich berechtigt ist, angemessene Alternativmaßnahmen zu ergreifen, solange das im DPA beschriebene allgemeine Sicherheitsniveau eingehalten wird.

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.

Bynder wählt seine Unterauftragsverarbeiter sehr sorgfältig aus, die alle strengen Sicherheitsbewertungen und -aufnahmen unterzogen werden. Bynder hat seinen Unterauftragsverarbeitern im Vertragsverhältnis zwischen dem Kunden und Bynder Datenschutzpflichten auferlegt, die den datenschutzrechtlichen Bestimmungen entsprechen. Unter Berücksichtigung der Stand der Technik, der Implementierungskosten und der Art der Verarbeitung werden unsere Unterauftragsverarbeiter angemessene technische und organisatorische Maßnahmen ergreifen, um personenbezogene Daten vor versehentlicher, unbefugter oder rechtswidriger Zerstörung, Verlust, Änderung, Offenlegung und Zugriff („Sicherheitsmaßnahmen“) zu schützen, gegebenenfalls einschließlich: (a) der Pseudonymisierung und Verschlüsselung personenbezogener Daten; (b) die Fähigkeit, die ständige Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme zu gewährleisten; (c) die Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls zeitnah wiederherzustellen; und (d) der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen zur Gewährleistung der Sicherheit der Verarbeitung hin sicherzustellen.

ANHANG III

ZUSÄTZLICHE KLAUSELN

Zur Klarstellung: Der Haftungsbeschränkungsabschnitt der Vereinbarung ist eine zusätzliche Klausel gemäß Klausel 2 dieser Klauseln.