Vertrag zur Auftragsverarbeitung (AVV) — Version 2.7

Stand: 21. November 2026. Für bestehende Nutzer wirksam ab 14. Dezember 2026 (Ziffer 11.3b). Die deutsche Fassung ist verbindlich; die englische Fassung dient der Information. Auftragsverarbeiter: Universal Exporters LLC, Houston, Texas, USA. Kontakt: ops@justarobot.online

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Zwischen dem Händler, der eine der in Anlage 1 genannten Apps nutzt und diesen Vertrag annimmt („Verantwortlicher"), **und** der Universal Exporters LLC, einer Limited Liability Company nach dem Recht des US-Bundesstaats Texas, 10006 Rolke Rd, Houston, TX 77099, USA, vertreten durch ihren Manager Bill S Vera („Auftragsverarbeiter").

1. Gegenstand, Dauer, Art und Zweck

1.1 Der Auftragsverarbeiter stellt die App(s) aus Anlage 1 bereit und verarbeitet dabei personenbezogene Daten im Auftrag des Verantwortlichen. Anlage 1 regelt je App Gegenstand, Art und Zweck, Datenarten, Kategorien betroffener Personen, Speicherort und Speicherdauer. 1.2 Dieser Vertrag gilt ab der Annahme, solange der Verantwortliche eine App nutzt, und danach bis zur Rückgabe oder Löschung der Daten nach Ziffer 9. 1.3 Nicht erfasst ist die Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters. Dazu gehören die eigenen Konto-, Kontakt- und Abrechnungsdaten des Verantwortlichen, die Zahlungsabwicklung über Stripe sowie Installationsnachweise und zusammengefasste Installationsstatistiken. Dafür gilt die Datenschutzerklärung des Auftragsverarbeiters. Support-Anfragen fallen unter diesen Vertrag, soweit sie Daten enthalten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen verarbeitet, etwa den Inhalt einer Problemmeldung.

2. Weisungen

2.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch bei Übermittlungen in ein Drittland, sofern nicht Unionsrecht oder das Recht eines Mitgliedstaats etwas anderes verlangt. In diesem Fall teilt er dies vorher mit, sofern das Recht dies nicht verbietet. 2.2 Weisungen sind dieser Vertrag und die vom Verantwortlichen gewählten Einstellungen der App. Weitere Weisungen erfolgen in Textform (E-Mail) an die Support-Adresse der jeweiligen App (Anlage 1). 2.3 Hält der Auftragsverarbeiter eine Weisung für datenschutzwidrig, teilt er dies unverzüglich mit und darf die Ausführung aussetzen, bis sie bestätigt oder geändert wird.

3. Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind. Derzeit ist das ausschließlich der Manager des Auftragsverarbeiters. Weitere Personen werden vor dem Zugriff schriftlich verpflichtet.

4. Sicherheit (Art. 32 DSGVO)

Der Auftragsverarbeiter trifft mindestens die technischen und organisatorischen Maßnahmen aus Anlage 2. Er darf sie weiterentwickeln, das Schutzniveau aber nicht senken.

5. Unterauftragsverarbeiter

5.1 Der Verantwortliche genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter. 5.2 **Neuer unmittelbarer Unterauftragsverarbeiter.** Der Auftragsverarbeiter informiert mindestens 30 Tage vor der Beauftragung eines zusätzlichen oder ersetzenden Unterauftragsverarbeiters. Die Information geht per E-Mail an die beim App-Plattformbetreiber hinterlegte Kontaktadresse und erscheint auch auf der Vertragsseite. Der Verantwortliche kann innerhalb dieser Frist aus berechtigten datenschutzrechtlichen Gründen in Textform widersprechen. 5.3 **Änderungen in der Kette eines Unterauftragsverarbeiters.** Anlage 3 verlinkt die Liste der Unterauftragsverarbeiter jedes Anbieters und dessen Ankündigungsfrist. Der Auftragsverarbeiter hat diese Mitteilungen abonniert. Er leitet eine Änderung innerhalb von 2 Werktagen nach Eingang weiter, in jedem Fall mindestens 7 Kalendertage vor ihrem Wirksamwerden, soweit die Frist des Anbieters das zulässt. 5.3a **Kurze Frist.** Lässt die Mitteilung eines Anbieters weniger als 7 Kalendertage, leitet der Auftragsverarbeiter sie sofort weiter und weist darauf hin. Der Verantwortliche kann dann auch nach dem Wirksamwerden widersprechen und nach Ziffer 5.4 kündigen. Zoho veröffentlicht keine feste Ankündigungsfrist; jede Zoho-Änderung gilt daher als kurzfristig. 5.4 **Ungelöster Widerspruch.** Widerspricht der Verantwortliche, versucht der Auftragsverarbeiter zunächst, den Widerspruch auszuräumen, etwa indem der Anbieter den neuen Unterauftragsverarbeiter nicht für die Daten des Verantwortlichen einsetzt, soweit der Anbieter das anbietet. Ist das nicht möglich, kann der Verantwortliche die Nutzung der betroffenen App mit sofortiger Wirkung beenden, vor oder nach dem Wirksamwerden der Änderung. Für die Zeit danach fällt keine Vergütung an; die Daten werden nach Ziffer 9 zurückgegeben oder gelöscht. Nach der Kündigung verarbeitet der Auftragsverarbeiter die Daten des Verantwortlichen nicht weiter über den abgelehnten Unterauftragsverarbeiter. 5.5 Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf ein Schutzniveau, das mindestens dem dieses Vertrags entspricht. Er haftet dem Verantwortlichen für seine Unterauftragsverarbeiter vollumfänglich (Art. 28 Abs. 4 DSGVO).

6. Ort der Verarbeitung und Übermittlung in Drittländer

6.1 Der Auftragsverarbeiter ist eine Gesellschaft mit Sitz in den USA. Datenbanken und Sicherungen liegen in der EU (Anlage 2). Soweit die Verarbeitung beim Auftragsverarbeiter eine Übermittlung der Daten des Verantwortlichen in ein Drittland ist, gelten dafür die Standardvertragsklauseln nach Anlage 4. 6.2 Einzelne Kopien liegen bei Unterauftragsverarbeitern außerhalb der EU. Über den E-Mail-Dienstleister versandte E-Mails werden in den USA gespeichert, ebenso das Support-Postfach (Anlage 3). Diese Übermittlungen stützen sich auf die Standardvertragsklauseln (Modul 3, Auftragsverarbeiter an Auftragsverarbeiter) im Auftragsverarbeitungsvertrag des jeweiligen Unterauftragsverarbeiters und zusätzlich auf das EU-U.S. Data Privacy Framework, soweit dieser zertifiziert ist. Eine Übermittlungsbewertung für jeden dieser Anbieter ist gesondert dokumentiert und auf Anfrage erhältlich. 6.3 Darüber hinaus verarbeitet der Auftragsverarbeiter die Daten des Verantwortlichen nicht außerhalb der EU/des EWR. Soll sich das ändern, kündigt er es wie eine Vertragsänderung an (Ziffer 11.4), und die Parteien vereinbaren vor Beginn ein wirksames Übermittlungsinstrument.

7. Rechte betroffener Personen und Unterstützung

7.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen nach Art. 12–22 DSGVO. Direkt eingehende Anträge leitet er unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst. 7.2 Speichert eine App personenbezogene Daten für den Verantwortlichen, stellt der Auftragsverarbeiter auf Anfrage innerhalb von 10 Werktagen einen Export der Daten zu einer benannten Person bereit oder löscht sie. 7.3 Er unterstützt den Verantwortlichen bei den Pflichten aus Art. 32–36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen.

8. Verletzungen des Schutzes personenbezogener Daten

8.1 Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes seiner personenbezogenen Daten unverzüglich nach Kenntnis. Eine erste Meldung erfolgt spätestens 48 Stunden nach Kenntnis, auch wenn der Sachverhalt noch nicht vollständig bekannt ist. 8.2 Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO. Weitere Angaben folgen schrittweise ohne weitere unangemessene Verzögerung (Art. 33 Abs. 4 DSGVO). 8.3 Die Meldung erfolgt per E-Mail an die Kontaktadresse des Verantwortlichen und, wo möglich, in der App. Der Auftragsverarbeiter dokumentiert jede Verletzung und die ergriffenen Maßnahmen.

9. Rückgabe und Löschung

9.1 **Wahlrecht.** Nach Ende der Leistungserbringung entscheidet der Verantwortliche, ob der Auftragsverarbeiter die für ihn gespeicherten personenbezogenen Daten zurückgibt oder löscht. 9.2 **Rückgabe.** Solange die App installiert ist, kann der Verantwortliche seine Daten jederzeit mit den Exportfunktionen der App sichern. Auf Anfrage in Textform stellt der Auftragsverarbeiter die für den Verantwortlichen gespeicherten Daten außerdem innerhalb von 10 Werktagen in einem gängigen maschinenlesbaren Format bereit, beschränkt auf den eigenen Shop und ohne Zugangsdaten.

- **Frist für die Anfrage:** Die Anfrage ist möglich, bis die Löschung nach Ziffer 9.3 durchgeführt ist, bei Shopify-Apps also mindestens 48 Stunden nach der Deinstallation, beim Kündigungsbutton und bei German Invoices 30 Tage. Die Einstellungsseite der App und die Vertragsseite weisen darauf hin.

- **Zurückstellung:** Geht die Anfrage nach der Deinstallation, aber vor der Löschung ein, stellt der Auftragsverarbeiter die Löschung bis zur Rückgabe zurück, höchstens 30 Tage.
- **Nach der Rückgabe:** Der Auftragsverarbeiter löscht alle verbleibenden Kopien nach Ziffer 9.3 bis 9.5 und bestätigt das (Ziffer 9.6).
- **Durchgeleitete Daten:** Daten, die eine App nur durchleitet und nicht speichert (Anlage 1), bestehen danach nicht mehr und können nicht zurückgegeben werden.

9.3 **Löschung.** Ohne Rückgabeverlangen löscht der Auftragsverarbeiter die gespeicherten personenbezogenen Daten:

- (a) **Shopify-Apps:** sobald die Löschaufforderung von Shopify eingeht (48 Stunden nach der Deinstallation), spätestens 7 Tage nach der Deinstallation, falls sie ausbleibt.
- (b) **Wix-Apps:** 48 Stunden nach der Entfernungsmeldung von Wix. Fehlt diese Meldung, prüft und löscht der Auftragsverarbeiter von Hand innerhalb von 14 Tagen, nachdem er es bemerkt hat.
- (c) **buchungsstapel.de:** sofort, wenn der Verantwortliche das Konto in den Einstellungen löscht. Lässt sich das Abonnement in diesem Moment nicht kündigen (Fehler beim Zahlungsdienstleister), wird nichts gelöscht; der Verantwortliche erhält einen Hinweis und kann es erneut versuchen. Eine Anfrage in Textform wird innerhalb von 30 Tagen umgesetzt.
- (d) **Vor dem 8. November 2026 entfernte Installationen:** Für sie gilt die automatische Rückfallregel nach (a) nicht. Der Auftragsverarbeiter prüft sie von Hand und löscht verbliebene Daten bis zum 31. Dezember 2026.
- (e) **Kündigungsbutton (Stripe App):** 30 Tage nach der Entfernungsmeldung von Stripe, damit die Rückgabe nach Ziffer 9.2 möglich bleibt. Fehlt diese Meldung, prüft und löscht der Auftragsverarbeiter von Hand innerhalb von 14 Tagen, nachdem er es bemerkt hat. Während der Nutzung gelten die Speicherfristen aus Anlage 1.
- (f) **German Invoices (Stripe App):** wie (e). Der Verantwortliche exportiert seine Belege vorher (Monatsexport in der App); die gesetzliche Aufbewahrung der Rechnungen ist seine eigene Pflicht und wird durch die Speicherung beim Auftragsverarbeiter nicht ersetzt.

9.4 **Sicherungen.** Nach der Löschung nach Ziffer 9.3 verbleiben gelöschte Daten nur bis zum regulären Ablauf in Sicherungen: 30 Tage, bei LUCID 7 Tage. Sicherungen dienen nur der Wiederherstellung des Betriebs. Wird eine Sicherung eingespielt, werden die seitdem erfolgten Löschungen vor der Wiederaufnahme des Betriebs erneut ausgeführt. 9.4a **Gesamtfristen.** Beim Auftragsverarbeiter selbst gespeicherte Kopien sind spätestens 37 Tage nach der Deinstallation gelöscht (LUCID: 14 Tage; Kündigungsbutton und German Invoices: 60 Tage). Ausnahmen:

- (i) eine Zurückstellung nach Ziffer 9.2 verlängert um bis zu 30 Tage;
- (ii) für Installationen nach Ziffer 9.3 (d) gilt diese Ziffer;
- (iii) für Kopien bei Unterauftragsverarbeitern gilt Ziffer 9.5.

9.5 **Kopien bei Unterauftragsverarbeitern.**

- **E-Mail-Dienstleister:** Über Resend versandte E-Mails einschließlich Inhalt verbleiben 30 Tage nach dem Versand in dessen Protokollen und verfallen dann. Resend bietet keine Löschung einzelner versandter E-Mails an. Erfordert der Löschantrag einer betroffenen Person eine frühere Löschung, beantragt der Auftragsverarbeiter sie bei Resend.
- **Support-Postfach:** Support-E-Mails und Problemmeldungen werden 24 Monate nach Abschluss des Supportfalls gelöscht. Der Auftragsverarbeiter führt diese Löschung monatlich durch.
- **Sicherungsspeicher:** wie Ziffer 9.4. 9.6 **Nachweis.** Auf Anfrage bestätigt der Auftragsverarbeiter die Löschung in Textform (Klausel 8.5 der Standardvertragsklauseln). 9.7 Gesetzliche Aufbewahrungspflichten nach Unionsrecht oder dem Recht eines Mitgliedstaats bleiben unberührt.

10. Nachweise und Kontrollen

10.1 Der Auftragsverarbeiter stellt alle zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlichen Informationen bereit. Dazu gehören dieser Vertrag mit Anlagen, schriftliche Antworten auf Fragen des Verantwortlichen in angemessener Frist und, soweit verfügbar, Nachweise über die Maßnahmen der Unterauftragsverarbeiter (etwa deren Zertifizierungen). 10.2 Der Verantwortliche oder ein von ihm beauftragter, zur Vertraulichkeit verpflichteter Prüfer kann Überprüfungen einschließlich Inspektionen durchführen. Diese finden in angemessenen Abständen statt, und jederzeit bei Anhaltspunkten für Verstöße, nach einer Verletzung des Schutzes personenbezogener Daten oder auf Verlangen einer Aufsichtsbehörde. Der Auftragsverarbeiter kann einen Prüfer vorschlagen; die Entscheidung trifft der Verantwortliche. 10.3 Inspektionen werden mit angemessener Frist angekündigt, in der Regel 30 Tage, kürzer, wenn der Anlass es erfordert. Sie finden zu Geschäftszeiten und ohne unverhältnismäßige Störung des Betriebs statt. Da der Auftragsverarbeiter keine für Besucher zugänglichen Räume unterhält, kann er stattdessen eine Prüfung aus der Ferne anbieten. Eine Vor-Ort-Inspektion bleibt möglich, wenn der Verantwortliche sie für erforderlich hält. 10.4 Jede Partei trägt ihre eigenen Kosten einer Überprüfung. 10.5 Der Auftragsverarbeiter unterstützt Prüfungen und Anfragen der zuständigen Aufsichtsbehörde.

11. Schlussbestimmungen

11.1 **Haftung.** Die Haftung zwischen den Parteien richtet sich nach den Nutzungsbedingungen der jeweiligen App, soweit gesetzlich zulässig. Diese Bedingungen beschränken weder Art. 82 DSGVO noch die Rechte betroffener Personen noch die Haftung nach Klausel 12 der Standardvertragsklauseln. 11.2 Bei Widersprüchen in Datenschutzfragen geht dieser Vertrag den Nutzungsbedingungen vor; die Standardvertragsklauseln gehen beiden vor (Anlage 4). 11.3 **Abschluss und Form.** Dieser Vertrag wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO), auf einem von zwei Wegen:

- eine befugte Person des Verantwortlichen setzt in der App das nicht vorausgewählte Häkchen zur Annahme und bestätigt; oder
- der Verantwortliche sendet ein unterschriebenes Exemplar zurück.

Der Auftragsverarbeiter speichert:

- Firma und Anschrift des Verantwortlichen, wie bei der Annahme angegeben;
- die Shop- oder Kontokennung der Plattform;
- Plattform-Benutzerkennung und Namen der annehmenden Person, mit ihrer Bestätigung, den Verantwortlichen vertreten zu dürfen;
- die erfassten Apps;
- die Version mit der SHA-256-Prüfsumme des genau angenommenen Dokuments;
- Datum und Uhrzeit.

Dieses Dokument kann der Verantwortliche jederzeit als PDF herunterladen.

11.3a **Neue Installationen.** Die Annahme ist Teil der Einrichtung. Vor der Annahme verarbeitet die App nur, was sie zur Anzeige der Einrichtung braucht: die Plattform-Sitzung sowie Name und Kontakt des Shops. Diese Verarbeitung ist durch die bei der Installation akzeptierten Nutzungsbedingungen und die Datenschutzerklärung gedeckt.

11.3b **Bestehende Nutzer.** Für bestehende Nutzer wird dieser Vertrag 30 Tage nach Ankündigung per E-Mail Bestandteil der Nutzungsbedingungen jeder App (Ziffer 11.4). Zusätzlich werden sie in der App um Annahme gebeten, die nach Ziffer 11.3 festgehalten wird. Die Funktionen der App laufen dabei unverändert weiter.

11.4 **Änderungen.** Änderungen dieses Vertrags kündigt der Auftragsverarbeiter mindestens 30 Tage vorher per E-Mail an. Eine Änderung, die den Schutz des Verantwortlichen verringert, wird erst nach erneuter Annahme wirksam; bis dahin gilt die angenommene Fassung weiter. Gesetzlich oder behördlich gebotene Änderungen können früher wirksam werden. 11.5 Ist eine Bestimmung unwirksam, bleibt der Vertrag im Übrigen wirksam.

Anlage 1 — Verarbeitung je App (Anhang I.B der Standardvertragsklauseln)

Für alle Apps gilt:

- **Zweck:** Bereitstellung der Funktionen der App auf Weisung des Verantwortlichen.
- **Art:** Lesen aus der Shop-Plattform oder dem Stripe-Konto des Verantwortlichen (beim Kündigungsbutton auch Ändern von Abonnements), Berechnen, Speichern wie angegeben, E-Mail-Versand wie angegeben.
- **Häufigkeit:** laufend während der Installation.
- **Besondere Kategorien:** keine.

- **Shopify-Sitzungen** nutzen Offline-Zugriffstoken. Die Felder für Name und E-Mail von Mitarbeitern existieren, bleiben aber in der Regel leer.

App (Support-Adresse)	Verarbeitete Daten	Beim Auftragsverarbeiter gespeichert und Dauer	Betroffene Personen
Export für DATEV / BMD-Export (Shopify), `support+datev@` / `support+bmd@`	**Aus Shopify gelesen während eines Exports:** Bestellungen, Erstattungen und Auszahlungen (Bestellnummer, Beträge, Steuer, Zielland). Kundennamen werden nicht gelesen; der Buchungstext enthält die Bestellnummer. **Kontakte:** Shop-Name und Kontakt-E-Mail; E-Mail des Steuerberaters, falls eingetragen.	**Bis zur Löschung nach Ziffer 9:** Einstellungen einschließlich Berater-/Mandantennummer, E-Mail des Steuerberaters und Link-Token, Exportverlauf (Zeitraum und Anzahlen), OSS-Steuersummen je Land, die Shopify-Sitzung. **Sicherungen:** 30 Tage. **E-Mails über Resend:** Steuerberater-Link (an den Steuerberater), Schwellenhinweise (an den Shop).	Kunden des Händlers (pseudonym über die Bestellnummer); Mitarbeiter des Händlers; Steuerberater
EU Compliance: Omnibus & GPSR (Shopify), `support+eucompliance@`	**Preise:** Produktpreise (nicht personenbezogen). **Produktdaten:** Produkttexte und GPSR-Angaben; vom Händler eingegebene Freitext-Notizen. **Widerrufsbutton:** Erklärungen (Name, E-Mail, Vertragsreferenz, Angaben, Datum und Uhrzeit, Seiten-URL). Sie laufen durch den Server, werden als Eintrag im eigenen Shop des Händlers gespeichert und als Eingangsbestätigung an den Kunden sowie als Hinweis an den Händler versandt, über Resend oder den eigenen SMTP-Server des Händlers.	**Speicherdauer:** Preisverlauf 400 Tage; Einstellungen bis zur Löschung, darunter Hinweisadresse, Absendername, Antwortadresse, Zusatztext und SMTP-Zugangsdaten (verschlüsselt, AES-256-GCM); die Shopify-Sitzung. **Erklärungen:** nicht in der Datenbank des Auftragsverarbeiters. **Sicherungen:** 30 Tage. **Kopien bei Resend:** siehe Ziffer 9.5.	Kunden des Händlers (Widerruf); Mitarbeiter des Händlers
EU Compliance Kit (Wix), `support+eucompliance-wix@`	**Widerrufserklärungen:** in einer Datensammlung auf der eigenen Wix-Website des Händlers; Bestätigungen über den Wix-E-Mail-Dienst des Händlers. Sie erreichen den Server des Auftragsverarbeiters nie. **GPSR-Kontaktdaten:** auf der Website des Händlers. **Server des Auftragsverarbeiters:** Produkt- und Variantenpreise, Website-URL und Instanz-ID.	**Preise und Website-Datensatz:** Löschung 48 Stunden nach Entfernung. **Installationsnachweis** (Website-URL, Daten): 3 Jahre. **Sicherungen:** 30 Tage.	Kunden des Händlers (nur auf der Website des Händlers); Händler
LUCID Verpackungsgesetz Report (Shopify), `support+epr@`	**Versandte Bestellungen:** Bestell-ID und -nummer, Zielland, Versand- und Stornodatum, Positionen (Produkt, Menge, Gewicht). Keine Namen, Anschriften oder E-Mail-Adressen.	**Bestelldaten und Einstellungen:** bis zur Löschung. **Zugriffsprotokoll** (wer Bestelldaten abgerufen hat): 12 Monate. **Sicherungen:** von der App verschlüsselt, 7 Tage.	Kunden des Händlers (pseudonym über die Bestellnummer); Mitarbeiter des Händlers
buchungsstapel.de (Web) + **WooCommerce-Plugin**, `support+stapel@`	**Hochgeladene Bestellexporte:** Kundennamen, Firma, Land, Beträge. Das Plugin entfernt E-Mail-Adressen vor dem Versand. Verarbeitung im Arbeitsspeicher, Verwerfung nach spätestens 30 Minuten, keine Speicherung auf Datenträger oder in der Datenbank. **Ergebnis:** Die erzeugte DATEV-Datei, die im Buchungstext Kundennamen enthält, geht per E-Mail über Resend an den Kontoinhaber; eine Kopie bleibt bei Resend (Ziffer 9.5). Auf Anforderung geht die Kontenzuordnung an eine vom Nutzer eingegebene Steuerberater-Adresse.	**Konto:** E-Mail, Stripe-Kundennummer, Abo-Status. **Anmeldeprotokoll:** E-Mail, IP-Adresse, Browser, 90 Tage. **Mandanten-Einstellungen und Exportverlauf:** nur Anzahlen. **Plattform-Anfragen:** E-Mail und Notiz. **Sicherungen:** 30 Tage.	Kunden des Händlers (Uploads im Arbeitsspeicher; Namen in der per E-Mail versandten DATEV-Datei); Händler; Steuerberater
Export für DATEV / BMD-Export / OSS Report (Wix), `support+datev-wix@` / `support+bmd-wix@` / `support+oss-wix@`	**Innerhalb von Wix gelesen während eines Exports oder einer OSS-Meldung:** Bestellungen, Erstattungen und Zahlungen; die Dateien werden im Dashboard heruntergeladen. **Auf der eigenen Wix-Website des Händlers:** Einstellungen (zum Beispiel Berater-/Mandantennummer, Konten, Land des Unternehmens) und OSS-Summen. **An den Auftragsverarbeiter:** Installations- und Entfernungsereignisse (App-ID, Ereignis, Instanz-ID). **Problemmeldungen** (auf Klick): Website-Name, Website-ID, E-Mail-Adresse der Website (als Antwortadresse), Seite und Zeitraum, angezeigte Fehlermeldung, Notiz des Händlers, ausgewählte Einstellungen, per E-Mail an den Support.	Auf Servern des Auftragsverarbeiters nichts außer dem Installationsnachweis und dem Nachweis über die Annahme dieses Vertrags (Ziffer 11.3); Problemmeldungen im Support-Postfach.	Kunden des Händlers (nur innerhalb von Wix); Händler
LUCID Report (Wix), `support+epr-wix@`	**Innerhalb von Wix gelesen, während eine Meldung berechnet wird:** Bestellungen und ihre Sendungen; ausgewertet werden Bestellnummer, Bestimmungsland, Versanddatum und Positionen (Produkt, Menge). Die Meldungen werden im Dashboard angezeigt und heruntergeladen. **Auf der eigenen Wix-Website des Händlers:** Verpackungen, Produktzuordnungen, Versandregeln, Einstellungen und abgeschlossene Zeiträume. **An den Auftragsverarbeiter:** Installations- und Entfernungsereignisse (App-ID, Ereignis, Instanz-ID).	Auf Servern des Auftragsverarbeiters nichts außer dem Installationsnachweis.	Kunden des Händlers (nur innerhalb von Wix); Händler
Kündigungsbutton (Stripe App), `support+kuendigung@`	**Kündigungserklärungen** über die vom Auftragsverarbeiter bereitgestellte Kündigungsseite des Händlers (§ 312k BGB): Art der Kündigung, Name, E-Mail-Adresse, gewählter Vertrag, gewünschter Beendigungszeitpunkt, bei außerordentlicher Kündigung der angegebene Grund, Datum und Uhrzeit des Eingangs, ein Hash der IP-Adresse (mit geheimem Schlüssel und Tagesdatum, zur Missbrauchsabwehr). **Widerrufserklärungen** über die vom Auftragsverarbeiter bereitgestellte Widerrufsseite des Händlers (§ 356a BGB): Name, E-Mail-Adresse, Angabe zum Vertrag, freiwillige weitere Angaben, gewählte Sprache, Datum und Uhrzeit des Eingangs, Status, ein Hash der IP-Adresse wie oben; im Stripe-Konto wird dafür nichts gelesen oder geändert. **Im Stripe-Konto des Händlers gelesen und geändert:** Kunden (Kundennummer, E-Mail-Adresse, Name) und Abonnements, um eine Kündigung zuzuordnen und auszuführen (Kündigungstermin und Metadaten am Abonnement, auch auf Anweisung im Dashboard); Produkte und Preise. **E-Mails über Resend:** Eingangsbestätigung (Kündigung und Widerruf), Bestätigung der Ausführung und gegebenenfalls der Rücknahme an den Kunden; Hinweise an die Hinweisadresse des Händlers.	**Erklärungen** (Kündigung und Widerruf) mit Zuordnung (Kunden- und Abonnement-IDs, Status, Beendigungsdatum): bis zum Ende des dritten Kalenderjahres nach Eingang (regelmäßige Verjährung), dann gelöscht; der IP-Hash nach 30 Tagen. **Einstellungen** (Firmenname, Links zu Logo, Impressum und Datenschutzerklärung, Hinweisadresse, Kündigungsfrist, angebotene Verträge) und das Stripe-Zugriffstoken (von der App verschlüsselt, AES-256-GCM): bis zur Löschung nach Ziffer 9. **Annahme dieses Vertrags** (Ziffer 11.3): Name und Stripe-Benutzerkennung der annehmenden Person. **Sicherungen:** 30 Tage. **Kopien bei Resend:** siehe Ziffer 9.5.	Kunden des Händlers (Kündigende, Widerrufende); Mitarbeiter des Händlers
German Invoices (Stripe App), `support+rechnung@`	**Im Stripe-Konto des Händlers gelesen:** bezahlte Checkout-Sitzungen (auch aus Payment Links) mit ihren Positionen: Name, Firma, E-Mail-Adresse, Rechnungsanschrift und USt-IdNr. des Käufers, Artikel, Beträge, Steuer, Kennungen der Sitzung und der Zahlung; Erstattungen; Produkte; Einstellungen der Payment Links. In Stripe wird nichts geändert. **Erstellt und gespeichert:** Rechnungen und Stornobelege zu diesen Zahlungen (PDF, bei inländischen Geschäftskunden als E-Rechnung) mit den genannten Käuferdaten; Zahlungen, die der Händler noch bearbeiten muss (Warteschlange), mit denselben Daten. **E-Mails über Resend:** der Beleg als Anhang an die E-Mail-Adresse des Käufers, wenn der Händler den Versand eingeschaltet hat.	**Belege** und die zugehörigen Zahlungsdaten: bis zum Ende des achten Kalenderjahres nach der Ausstellung, dann gelöscht; früher bei Löschung nach Ziffer 9. **Zahlungen ohne Beleg:** in der Warteschlange bis zur Bearbeitung durch den Händler, längstens 12 Monate nach der Zahlung; übersprungene oder vom Händler geschlossene 90 Tage nach dem Überspringen bzw. Schließen. **Einstellungen** (Firmendaten für die Rechnung, Steuerart, Nummernkreis) und das Stripe-Zugriffstoken (von der App verschlüsselt, AES-256-GCM): bis zur Löschung nach Ziffer 9. **Annahme dieses Vertrags** (Ziffer 11.3): Name und Stripe-Benutzerkennung der annehmenden Person. **Sicherungen:** 30 Tage. **Kopien bei Resend:** siehe Ziffer 9.5.	Kunden des Händlers (Käufer); Mitarbeiter des Händlers

Parteien

- **Datenexporteur:** der Verantwortliche, mit Name, Anschrift und Kontakt, wie bei der Annahme beim App-Plattformbetreiber hinterlegt. Rolle: Verantwortlicher. Tätigkeiten: gemäß Anlage 1.
- **Datenimporteur:** Universal Exporters LLC, Anschrift wie oben. Kontakt: ops@justarobot.online. Rolle: Auftragsverarbeiter.

Die Unterzeichnung erfolgt durch die Annahme nach Ziffer 11.3.

Zuständige Aufsichtsbehörden Für den Verantwortlichen: die Behörde seines Mitgliedstaats. Für den Auftragsverarbeiter: die Behörde, die für den Verantwortlichen zuständig ist (Anlage 4, Klausel 13).

Anlage 2 — Technische und organisatorische Maßnahmen (Anhang II)

- **Standort.** Anwendungsserver und Datenbanken bei Railway in der Region europe-west4 (Amsterdam), am 8. November 2026 für jeden Dienst aus Anlage 1 geprüft, für den Kündigungsbutton am 14. November 2026, für German Invoices vor dem ersten Einsatz. Sicherungen bei Cloudflare R2 mit EU-Jurisdiktion (der Sicherungs-Endpunkt jedes Dienstes ist der EU-Endpunkt, geprüft am 8. November 2026).
- **Kopien außerhalb der EU.** Über Resend versandte E-Mails werden in den USA gespeichert. Das Support-Postfach bei Zoho liegt in den USA; der Wechsel in Zohos EU-Rechenzentrum wurde am 8. November 2026 beantragt und steht aus. Sonst wird nichts außerhalb der EU gespeichert.
- **Verschlüsselung bei der Übertragung.** TLS für jede Verbindung.
- **Verschlüsselung im Ruhezustand.** Anbieterseitige Verschlüsselung für Datenbanken und Sicherungen. Sicherungen von LUCID, Kündigungsbutton und German Invoices werden zusätzlich von der App verschlüsselt (AES-256-GCM, Schlüssel außerhalb des Sicherungsspeichers). SMTP-Passwörter der Händler und die Stripe-Zugriffstoken des Kündigungsbuttons und von German Invoices werden von der App verschlüsselt (AES-256-GCM).
- **Zugriffskontrolle.** Produktivsysteme und Anbieterkonten sind nur dem Manager zugänglich. Starke individuelle Passwörter; Zwei-Faktor-Authentifizierung auf allen Anbieterkonten (Railway, Cloudflare, Resend, Shopify Partners, Wix, GitHub, Zoho und Stripe). Die Shopify-Zugriffstoken der Shops liegen in der Datenbank, vom Anbieter im Ruhezustand verschlüsselt.
- **Datensparsamkeit.**
  - Hochgeladene oder gelesene Bestelldaten werden im Arbeitsspeicher verarbeitet, wo die Funktion es erlaubt (Anlage 1). Ergebnisse werden nur dort per E-Mail versandt, wo Anlage 1 es nennt; dann bleibt eine Kopie beim E-Mail-Dienstleister.
  - Export für DATEV liest keine Kundennamen.
  - Das WooCommerce-Plugin entfernt E-Mail-Adressen vor dem Upload.
  - LUCID speichert keine Namen oder Anschriften.
  - Der Kündigungsbutton speichert von der IP-Adresse nur einen Hash, und diesen 30 Tage.
- **Protokollierung.**
  - Server-Protokolle enthalten Shop-Kennungen, Fehlermeldungen und Anfragepfade, keine Kundendaten (eine verbleibende Protokollzeile in EU Compliance wird ab 12. November 2026 durch einen Hash-Verweis ersetzt).
  - Fehlermeldungen an den Manager enthalten keine Shop-Domain, E-Mail-Adresse oder lange IDs; der vollständige Kontext bleibt im Server-Protokoll.
  - Aufbewahrung der Server-Protokolle: 7 Tage (Railway-Tarif Hobby).
- **Verfügbarkeit.** Laufende Datenbankreplikation (Litestream, im Sekundentakt) oder eine nächtliche Sicherung (LUCID, Kündigungsbutton, German Invoices). Dienste mit Litestream starten nicht mit einer leeren Datenbank, damit Daten nicht versehentlich überschrieben werden.
- **Löschung.**
  - Nach Ziffer 9.
  - Preisverlauf: 400 Tage (Shopify) bzw. der eingestellte Zeitraum (Wix).
  - Anmeldeprotokoll: 90 Tage. Zugriffsprotokoll: 12 Monate.
  - Sicherungen: 30 Tage (LUCID 7).
- **Überwachung und Vorfälle.** Automatische Fehler- und Verfügbarkeitsüberwachung mit Benachrichtigung des Managers rund um die Uhr; Umgang mit Verletzungen nach Ziffer 8.
- **Unterauftragsverarbeiter.** Auswahl nach Auftragsverarbeitungsvertrag und Übermittlungsinstrument (Anlage 3); Prüfung bei jeder Änderungsmitteilung.

Anlage 3 — Unterauftragsverarbeiter (Anhang III)

Keine Unterauftragsverarbeiter sind:

- **Shopify und Wix.** Das sind die eigenen Plattformen des Verantwortlichen, mit dessen eigenem Vertrag. Bestätigungen der Wix-App laufen über den eigenen Wix-E-Mail-Dienst des Verantwortlichen.
- **Stripe.** Stripe verarbeitet nur die eigenen Abrechnungsdaten des Auftragsverarbeiters. Der Kündigungsbutton und German Invoices arbeiten im eigenen Stripe-Konto des Verantwortlichen; dort ist Stripe dessen eigener Dienstleister, mit dessen eigenem Vertrag.
- **GitHub.** Dort liegen keine personenbezogenen Daten.

Unterauftragsverarbeiter	Anschrift	Zweck / Apps	Datenstandort	Übermittlungsinstrument	Eigene Liste / Frist	AV-Vertrag
Railway Corporation	548 Market St PMB 68956, San Francisco, CA 94104, USA	Betrieb von Anwendung und Datenbank; alle Apps aus Anlage 1 außer den Wix-Apps Export für DATEV, BMD-Export, OSS Report und LUCID Report	EU (Amsterdam, europe-west4)	Standardvertragsklauseln Modul 3 (Railway-AVV; Klausel 9 Option 1 mit 10 Tagen Ankündigung); DPF als Alternative	https://trust.railway.com/item/subprocessors — 10 Tage	https://railway.com/legal/dp
Cloudflare, Inc.	101 Townsend Street, San Francisco, CA 94107, USA	Sicherungsspeicher (R2) für DATEV/BMD, EU Compliance (Shopify und Wix-Server), LUCID, buchungsstapel.de, Kündigungsbutton, German Invoices	EU (R2 mit EU-Jurisdiktion)	Standardvertragsklauseln Modul 2/3 (Cloudflare-AVV Ziff. 6.2); EU-U.S. DPF	https://www.cloudflare.com/gdpr/subprocessors/ — 30 Tage	https://www.cloudflare.com customer-dpa/
Plus Five Five, Inc. („Resend“)	2261 Market Street #5039, San Francisco, CA 94114, USA	E-Mail-Versand: Widerrufs- und Kündigungsbestätigungen und Hinweise, Rechnungen und Stornobelege an Käufer, Steuerberater-Links, Schwellenhinweise, Anmeldelinks, DATEV-Dateien an den Kontoinhaber, Problemmeldungen	Versand aus der EU-Region (Irland, eu-west-1); Speicherung in den USA	Standardvertragsklauseln Modul 2/3 (Resend-AVV Ziff. 6.2, als unterzeichnet geltend); EU-U.S. DPF (Rezertifizierung in Prüfung, Stand Nov. 2026)	https://resend.com/legal/subprocessors — 14 Tage	https://resend.com/legal/dp
Zoho Corporation GmbH (Vertragspartner für Konten in Deutschland; Kontoland ist Deutschland)	laut https://www.zoho.com/legal/zoho-contracting-entities.html	Support-Postfach (Anfragen und Problemmeldungen, die Shopdaten enthalten können)	USA (Rechenzentrum zoho.com); Wechsel ins EU-Rechenzentrum am 8. November 2026 beantragt	Standardvertragsklauseln laut Zoho-AVV, am 8. November 2026 bei legal@zohocorp.com angefordert	https://www.zoho.com/privacy/sub-processors.html — keine feste Frist; Änderungsmitteilungen per Abonnement (gilt als kurzfristig, Ziffer 5.3a)	auf Anfrage (legal@zohoco

Anlage 4 — Standardvertragsklauseln (Modul 2)

Diese Anlage gilt, soweit die Verarbeitung beim Auftragsverarbeiter eine Übermittlung personenbezogener Daten in ein Drittland ist (Ziffer 6.1). Insoweit vereinbaren die Parteien die Standardvertragsklauseln nach dem Durchführungsbeschluss (EU) 2021/914, Modul 2 (Verantwortlicher an Auftragsverarbeiter), wie folgt:

- **Angaben:** aus den Anlagen 1–3.
- **Text:** der amtliche Text ist der PDF-Fassung beigefügt.

- **Klausel 7 (Kopplungsklausel):** gilt.
- **Klausel 9 Buchst. a:** Option 2, allgemeine schriftliche Genehmigung, Ankündigung wie in Ziffer 5.
- **Klausel 11 Buchst. a:** Die optionale unabhängige Streitbeilegungsstelle wird nicht gewählt.
- **Klausel 13:** die Aufsichtsbehörde des Mitgliedstaats des Datenexporteurs.
- **Klausel 17:** Option 2, das Recht des Mitgliedstaats des Datenexporteurs; ersatzweise Irland.
- **Klausel 18 Buchst. b:** die Gerichte des Mitgliedstaats des Datenexporteurs.
- **Widersprüche:** Bei Widersprüchen gehen die Klauseln vor.

Unterliegt die Verarbeitung des Auftragsverarbeiters selbst der DSGVO, passen diese Klauseln nach Auffassung der Kommission nicht (SCC-Fragen und Antworten); sie gelten dann als vertragliche Garantie, bis die Kommission Klauseln für diesen Fall erlässt, die der Auftragsverarbeiter dann stattdessen anbietet.

Data Processing Agreement — Version 2.7 (English, for information)

Version of 21 November 2026. For existing users effective from 14 December 2026 (clause 11.3b). The German version is binding.

Data Processing Agreement under Art. 28 GDPR

Between the merchant that uses one of the apps in Annex 1 and accepts this agreement ("Controller") **and** Universal Exporters LLC, a Texas limited liability company, 10006 Rolke Rd, Houston, TX 77099, USA, represented by its Manager Bill S Vera ("Processor").

1. Subject, duration, nature and purpose

1.1 The Processor provides the app(s) in Annex 1 and, in doing so, processes personal data on behalf of the Controller. Annex 1 sets out per app the subject, nature and purpose, the types of personal data, the categories of data subjects, where data is stored and how long it is kept. 1.2 This agreement applies from acceptance for as long as the Controller uses an app, and afterwards until the data has been returned or deleted under clause 9. 1.3 Processing for the Processor's own purposes is not covered by this agreement. That includes the Controller's own account, contact and billing data, payment data processed by Stripe, and install records and aggregated install statistics. The Processor's privacy policy governs that processing. Support requests are covered by this agreement insofar as they contain data the Processor processes on the Controller's behalf, such as the contents of a problem report.

2. Instructions

2.1 The Processor processes personal data only on documented instructions from the Controller, including with regard to transfers to a third country, unless Union or Member State law requires otherwise. In that case the Processor informs the Controller beforehand, unless the law prohibits it. 2.2 The instructions are this agreement and the settings the Controller chooses in the app. Further instructions are given in text form (e-mail) to the support address of the respective app (Annex 1). 2.3 If the Processor considers an instruction to infringe data protection law, it informs the Controller without delay and may suspend that instruction until it is confirmed or changed.

3. Confidentiality

The Processor ensures that every person authorised to process the personal data is bound to confidentiality. Today that is only the Processor's Manager. Any further person is bound in writing before receiving access.

4. Security (Art. 32 GDPR)

The Processor implements at least the technical and organisational measures in Annex 2. It may develop them further but may not lower the level of protection.

5. Sub-processors

5.1 The Controller authorises the sub-processors listed in Annex 3. 5.2 **New direct sub-processor.** The Processor informs the Controller at least 30 days before engaging an additional or replacement sub-processor. Notice goes by e-mail to the contact address the Controller has stored with the app platform and is also shown on the agreement page. The Controller may object in text form within that period on reasonable data protection grounds. 5.3 **Changes in a sub-processor's own chain.** Annex 3 links each sub-processor's own list of sub-processors and the notice period that sub-processor gives. The Processor subscribes to those notices. It forwards a change to the Controller within 2 working days of receiving it, and in any case at least 7 calendar days before the change takes effect, as long as the provider's own notice allows that. 5.3a **Short notice.** If a provider's notice leaves less than 7 calendar days, the Processor forwards it at once and says so. The Controller may then object and terminate under clause 5.4 even after the change has taken effect. Zoho publishes no fixed notice period, so a Zoho change is always treated as short notice. 5.4 **Unresolved objection.** If the Controller objects, the Processor first tries to resolve the objection, for example by having the provider not use the new sub-processor for the Controller's data where the provider offers that. If that is not possible, the Controller may terminate use of the affected app with immediate effect, before or after the change takes effect. No fee applies for the period after termination, and data is returned or deleted under clause 9. The Processor does not continue to process the Controller's data through the sub-processor objected to once the Controller has terminated. 5.5 The Processor imposes on each sub-processor, by contract, data protection obligations that offer at least the protection of this agreement. It remains fully liable to the Controller for its sub-processors (Art. 28(4) GDPR).

6. Place of processing and transfers to third countries

6.1 The Processor is a company based in the USA. The databases and backups are stored in the EU (Annex 2). To the extent that processing by the Processor is a transfer of the Controller's data to a third country, the standard contractual clauses in Annex 4 apply to it. 6.2 Some copies are held by sub-processors outside the EU. E-mails sent through the e-mail sub-processor are stored in the USA, and so is the support mailbox (Annex 3). These transfers rely on the standard contractual clauses (Module Three, processor to processor) in that sub-processor's data processing agreement, and additionally on the EU-US Data Privacy Framework where the sub-processor is certified. A transfer assessment for each of these providers is documented separately and available on request. 6.3 The Processor does not process the Controller's data outside the EU/EEA in any other way. If that is ever to change, the Processor announces it like a change to this agreement (clause 11.4), and the parties agree a valid transfer tool before it starts.

7. Data subject rights and assistance

7.1 The Processor assists the Controller with appropriate technical and organisational measures, insofar as possible, in responding to requests from data subjects under Art. 12–22 GDPR. A request that reaches the Processor directly is forwarded to the Controller without undue delay and not answered by the Processor itself. 7.2 Where an app stores personal data for the Controller, the Processor provides on request, within 10 working days, an export of the data concerning a named data subject, or deletes it. 7.3 The Processor assists the Controller with Art. 32–36 GDPR (security, breach notification, impact assessments, prior consultation), taking into account the nature of processing and the information available to it.

8. Personal data breaches

8.1 The Processor notifies the Controller of a personal data breach concerning the Controller's data without undue delay after becoming aware of it. An initial notice goes out at the latest 48 hours after becoming aware, even if the facts are not yet complete. 8.2 The notice contains, as far as known, the information under Art. 33(3) GDPR. Further information follows in phases without undue further delay (Art. 33(4)). 8.3 Notice goes by e-mail to the Controller's contact address, and in the app where possible. The Processor documents every breach and the measures taken.

9. Return and deletion

9.1 **Choice.** At the end of the provision of services, the Controller chooses whether the Processor returns or deletes the personal data it stores for the Controller. 9.2 **Return.** While the app is installed, the Controller can export its data with the app's export functions at any time. On a request in text form, the Processor also provides the data stored for the Controller in a common machine-readable format within 10 working days. That data is limited to the Controller's own store and excludes access credentials.

- **When to ask:** the request can be made until the deletion under clause 9.3 has been carried out. For Shopify apps that is at least 48 hours after uninstall; for the Kündigungsbutton and German Invoices, 30 days. The app's settings page and the agreement page point this out.
- **Hold:** if the request arrives after uninstall but before deletion, the Processor holds the deletion until the data has been returned, for at most 30 days.
- **After return:** the Processor deletes all remaining copies under clauses 9.3–9.5 and confirms this (clause 9.6).
- **Pass-through data:** data that an app only passes through without storing it (Annex 1) does not exist afterwards and cannot be returned.

9.3 **Deletion.** Without a return request, the Processor deletes the stored personal data as follows:

- (a) **Shopify apps:** when Shopify's deletion request arrives (sent 48 hours after uninstall), and at the latest 7 days after uninstall if that request does not arrive.

- (b) **Wix apps:** 48 hours after Wix reports the removal. If that report is missing, the Processor checks and deletes by hand within 14 days of noticing it.
- (c) **buchungsstapel.de:** at once when the Controller deletes the account in its settings. If the subscription cannot be cancelled at that moment (a payment provider error), nothing is deleted, and the Controller sees a message and can retry. A request in text form is carried out within 30 days.
- (d) **Installations removed before 8 Nov 2026:** these do not have the automatic fallback under (a). The Processor checks them by hand and deletes what is left by 31 Dec 2026.
- (e) **Kündigungsbutton (Stripe App):** 30 days after Stripe reports the removal, so that a return under clause 9.2 remains possible. If that report is missing, the Processor checks and deletes by hand within 14 days of noticing it. While the app is in use, the retention periods of Annex 1 apply.
- (f) **German Invoices (Stripe App):** as (e). The Controller exports its documents beforehand (month export in the app); keeping invoices for the statutory period is the Controller's own duty, which storage at the Processor does not replace.

9.4 **Backups.** After deletion under clause 9.3, deleted data remains in backups only until they expire on their normal cycle: 30 days, or 7 days for LUCID. Backups are used only to restore operation. If a backup is restored, deletions made since then are applied again before normal operation resumes. 9.4a **Overall periods.** Copies held by the Processor itself are gone at the latest 37 days after uninstall (LUCID: 14 days; Kündigungsbutton and German Invoices: 60 days). Exceptions:

- (i) a return hold under clause 9.2 adds up to 30 days;
- (ii) installations under clause 9.3(d) follow that clause;
- (iii) copies at sub-processors follow clause 9.5.

9.5 **Copies at sub-processors.**

- **E-mail sub-processor:** e-mails sent through Resend, including content, are kept in its logs for 30 days after sending and then expire. Resend offers no deletion of a single sent e-mail. Where a data subject's erasure request needs earlier deletion, the Processor asks Resend for it.
- **Support mailbox:** support e-mails and problem reports are deleted 24 months after the support case was closed. The Processor runs this deletion monthly.
- **Backup storage:** as in clause 9.4. 9.6 **Proof.** On request, the Processor confirms deletion in text form (SCC Clause 8.5). 9.7 Retention required by Union or Member State law remains unaffected.

10. Information and audits

10.1 The Processor makes available all information necessary to demonstrate compliance with Art. 28 GDPR. This includes this agreement and its annexes, written answers to the Controller's questions within a reasonable period, and evidence of sub-processors' measures (for example, their certifications) where available. 10.2 The Controller, or an auditor it mandates who is bound to confidentiality, may carry out audits, including inspections. Audits take place at reasonable intervals, and at any time where there are indications of non-compliance, after a personal data breach, or where a supervisory authority requests it. The Processor may suggest an auditor; the Controller decides. 10.3 Inspections are announced with reasonable notice, normally 30 days, shorter where the reason for the audit requires it. They take place during business hours and without disproportionate disruption of operations. As the Processor has no premises open to visitors, it may offer a remote inspection instead; an on-site inspection remains possible where the Controller considers it necessary. 10.4 Each party bears its own costs of an audit. 10.5 The Processor supports audits and requests by the competent supervisory authority.

11. Final provisions

11.1 **Liability.** Liability between the parties follows the terms of service of the respective app, as far as the law permits. Nothing in those terms limits Art. 82 GDPR, the rights of data subjects, or the liability under Clause 12 of the standard contractual clauses. 11.2 Where this agreement and the terms of service conflict on data protection, this agreement prevails; the standard contractual clauses prevail over both (Annex 4). 11.3 **Conclusion and form.** This agreement is concluded in electronic form (Art. 28(9) GDPR) in one of two ways:

- an authorised person of the Controller ticks the acceptance box in the app, which is not pre-ticked, and confirms; or
- the Controller returns a signed copy.

The Processor records:

- the Controller's legal name and address, as entered at acceptance;
- the platform store or account identifier;
- the accepting person's platform user id and name, with their confirmation that they may bind the Controller;
- the apps covered;
- the version, with the SHA-256 checksum of the exact document accepted;
- the date and time.

The Controller can download that exact document as a PDF at any time.

11.3a **New installations.** Acceptance is part of setup. Before acceptance, the app processes only what it needs to show the setup: the platform session and the store's name and contact. That processing is covered by the terms of service and privacy policy accepted at installation.

11.3b **Existing users.** For existing users, this agreement becomes part of each app's terms of service 30 days after notice by e-mail (clause 11.4). They are also asked to accept it in the app, which records their acceptance under clause 11.3. The app's functions continue throughout.

11.4 **Changes.** The Processor announces changes to this agreement at least 30 days in advance by e-mail. A change that reduces the Controller's protection takes effect only after renewed acceptance. Until then the accepted version continues to apply. Changes required by law or by a supervisory authority may take effect earlier. 11.5 If a provision is invalid, the remainder stays valid.

Annex 1 — Processing per app (SCC Annex I.B)

Common to all apps:

- **Purpose:** providing the app's functions at the Controller's instruction.
- **Nature:** reading from the Controller's store platform or Stripe account (for the Kündigungsbutton also changing subscriptions), computing, storing as stated, and sending e-mails as stated.
- **Frequency:** continuous while installed.
- **Special categories:** none.
- **Shopify sessions** use offline access tokens. The staff name and e-mail fields exist but are normally empty.

App (support address)	Data processed	Stored by the Processor, and how long	Data subjects
Export für DATEV / BMD-Export (Shopify), `support+datev@` / `support+bmd@`	**Read from Shopify during an export:** orders, refunds and payouts (order number, amounts, tax, destination country). Customer names are not read; the booking text carries the order number. **Contacts:** shop name and contact e-mail; the accountant's e-mail if entered.	**Kept until deletion under clause 9:** settings including Berater-/Mandantennummer, the accountant e-mail and a link token, export history (period and counts), OSS VAT totals per country, the Shopify session. **Backups:** 30 days. **E-mails via Resend:** the accountant link (to the accountant), threshold notices (to the shop).	Merchant's customers (pseudonymous via order number); merchant's staff; accountant
EU Compliance: Omnibus & GPSR (Shopify), `support+eucompliance@`	**Prices:** product prices (not personal). **Product data:** product texts and GPSR data; free-text notes entered by the merchant. **Withdrawal button:** declarations (name, e-mail, contract reference, details, date and time, page URL). They pass through the server, are stored as an entry in the merchant's own store, and are sent as an acknowledgement to	**Retention:** price history 400 days; settings until deletion, including the notice address, sender name, reply-to, extra text and SMTP credentials (encrypted, AES-256-GCM); the Shopify	Merchant's customers (withdrawal); merchant's staff

App (support address)	Data processed	Stored by the Processor, and how long	Data subjects
	the customer and a notice to the merchant, via Resend or the merchant's own SMTP server.	session. **Declarations:** not in the Processor's database. **Backups:** 30 days. **Resend copies:** see clause 9.5.	
EU Compliance Kit (Wix), `support+eucompliance-wix@`	**Withdrawal declarations:** stored in a data collection on the merchant's own Wix site, with acknowledgements sent through the merchant's Wix e-mail service. These never reach the Processor's server. **GPSR contact data:** stored on the merchant's site. **Processor's server:** product and variant prices, the site URL and the instance id.	**Prices and site record:** deleted 48 hours after removal. **Install record** (site URL, dates): 3 years. **Backups:** 30 days.	Merchant's customers (on the merchant's site only); merchant
LUCID Verpackungsgesetz Report (Shopify), `support+epr@`	**Shipped orders:** order id and number, destination country, ship and cancel dates, line items (product, quantity, weight). No names, addresses or e-mails.	**Order records and settings:** kept until deletion. **Access log** (who read order data): 12 months. **Backups:** encrypted by the app, 7 days.	Merchant's customers (pseudonymous via order number); merchant's staff
buchungsstapel.de (web) + **WooCommerce plugin**, `support+stapel@`	**Uploaded order exports:** customer names, company, country, amounts. The plugin removes e-mail addresses before sending. Parsed in memory, discarded after at most 30 minutes, never written to disk or the database. **Output:** the generated DATEV file, which contains customer names in the booking text, is e-mailed via Resend to the account owner, so a copy stays at Resend (clause 9.5). On request, the account mapping is mailed to an accountant address the user enters.	**Account:** e-mail, Stripe customer id, subscription status. **Login log:** e-mail, IP address, browser, kept 90 days. **Mandant settings and export history:** counts only. **Platform requests:** e-mail and note. **Backups:** 30 days.	Merchant's customers (uploads in memory; names in the e-mailed DATEV file); merchant; accountant
Export für DATEV / BMD-Export / OSS Report (Wix), `support+datev-wix@` / `support+bmd-wix@` / `support+oss-wix@`	**Read inside Wix during an export or an OSS report:** orders, refunds and payments; the files are downloaded in the dashboard. **On the merchant's own Wix site:** settings (for example Berater-/Mandantennummer, accounts, country of the business) and OSS totals. **To the Processor:** install and removal events (app id, event, instance id). **Problem reports** (on click): site name, site id, the site's e-mail address (as the reply address), page and period, the error message shown, the merchant's note, selected settings, by e-mail to support.	Nothing on the Processor's servers beyond the install record and the record of this agreement's acceptance (clause 11.3); problem reports in the support mailbox.	Merchant's customers (inside Wix only); merchant
LUCID Report (Wix), `support+epr-wix@`	**Read inside Wix while a report is computed:** orders and their fulfilments; the app evaluates order number, destination country, ship date and line items (product, quantity). Reports are shown and downloaded in the dashboard. **On the merchant's own Wix site:** packaging, product assignments, shipping rules, settings and closed periods. **To the Processor:** install and removal events (app id, event, instance id).	Nothing on the Processor's servers beyond the install record.	Merchant's customers (inside Wix only); merchant
Kündigungsbutton (Stripe App), `support+kuendigung@`	**Cancellation declarations** through the merchant's cancellation page provided by the Processor (§ 312k BGB): type of cancellation, name, e-mail address, chosen contract, requested end date, the reason given for an extraordinary cancellation, date and time of receipt, a hash of the IP address (keyed with a secret and the date, for abuse prevention). **Withdrawal declarations** through the merchant's withdrawal page provided by the Processor (§ 356a BGB): name, e-mail address, what identifies the contract, optional further details, chosen language, date and time of receipt, status, a hash of the IP address as above; nothing is read or changed in the Stripe account for them. **Read and changed in the merchant's Stripe account:** customers (customer id, e-mail address, name) and subscriptions, to match and carry out a cancellation (cancellation date and metadata on the subscription, also on instruction in the Dashboard); products and prices. **E-mails via Resend:** acknowledgement (cancellation and withdrawal), confirmation of execution and, where applicable, of reversal to the customer; notices to the merchant's notice address.	**Declarations** (cancellation and withdrawal) with their match (customer and subscription ids, status, end date): until the end of the third calendar year after receipt (regular limitation period), then deleted; the IP hash after 30 days. **Settings** (company name, links to logo, Impressum and privacy policy, notice address, notice period, offered contracts) and the Stripe access token (encrypted by the app, AES-256-GCM): until deletion under clause 9. **Acceptance of this agreement** (clause 11.3): name and Stripe user id of the accepting person. **Backups:** 30 days. **Resend copies:** see clause 9.5.	Merchant's customers (cancelling, withdrawing); merchant's staff
German Invoices (Stripe App), `support+rechnung@`	**Read in the merchant's Stripe account:** paid Checkout Sessions (also from Payment Links) with their line items: the buyer's name, company, e-mail address, billing address and VAT ID, items, amounts, tax, the ids of the session and the payment; refunds; products; Payment Link settings. Nothing is changed in Stripe. **Created and stored:** invoices and cancellation documents for these payments (PDF, as an e-invoice for domestic business buyers) with the buyer data named above; payments the merchant still has to deal with (queue), with the same data. **E-mails via Resend:** the document as an attachment to the buyer's e-mail address, if the merchant has switched sending on.	**Documents** and the payment data belonging to them: until the end of the eighth calendar year after issue, then deleted; earlier on deletion under clause 9. **Payments without a document:** in the queue until the merchant deals with them, at most 12 months after the payment; payments skipped or closed by the merchant, 90 days after the skip or close. **Settings** (company data for the invoice, tax mode, number range) and the Stripe access token (encrypted by the app, AES-256-GCM): until deletion under clause 9. **Acceptance of this agreement** (clause 11.3): name and Stripe user id of the accepting person. **Backups:** 30 days. **Resend copies:** see clause 9.5.	Merchant's customers (buyers); merchant's staff

Parties

- **Data exporter:** the Controller, with its name, address and contact as stored with the app platform at acceptance. Role: controller. Activities: those in Annex 1.
- **Data importer:** Universal Exporters LLC, address above. Contact: ops@justarobot.online. Role: processor.

The parties sign by acceptance under clause 11.3.

Competent supervisory authorities For the Controller: the authority of its own Member State. For the Processor: the authority competent for the Controller (Annex 4, clause 13).

Annex 2 — Technical and organisational measures (SCC Annex II)

- **Location.** Application servers and databases at Railway in region europe-west4 (Amsterdam), verified on 8 Nov 2026 for every service in Annex 1, for the Kündigungsbutton on 14 Nov 2026, for German Invoices before first use. Backups at Cloudflare R2 with EU jurisdiction (every service's backup endpoint is the EU-jurisdiction endpoint, verified 8 Nov 2026).
- **Copies outside the EU.** E-mails sent through Resend are stored in the USA. The support mailbox at Zoho is in the USA; the move to Zoho's EU data centre was requested on 8 Nov 2026 and is pending. Nothing else is stored outside the EU.
- **Encryption in transit.** TLS for every connection.
- **Encryption at rest.** Provider-side encryption for databases and backups. LUCID, Kündigungsbutton and German Invoices backups are additionally encrypted by the app (AES-256-GCM, key kept outside the backup storage). Merchant SMTP passwords and the Stripe access tokens of the Kündigungsbutton and German Invoices are encrypted by the app (AES-256-GCM).
- **Access control.** Production systems and provider accounts are accessible only to the Manager. Strong individual passwords; two-factor authentication on all provider accounts (Railway, Cloudflare, Resend, Shopify Partners, Wix, GitHub, Zoho and Stripe). The Shopify access tokens of the stores are held in the database, encrypted at rest by the provider.
- **Data minimisation.**
  - Uploaded or read order data is processed in memory where the function allows (Annex 1). Results are e-mailed only where Annex 1 says so, which leaves a copy at the e-mail sub-processor.
  - Export für DATEV does not read customer names.
  - The WooCommerce plugin removes e-mail addresses before upload.
  - LUCID stores no names or addresses.
  - The Kündigungsbutton stores only a hash of the IP address, and that for 30 days.
- **Logging.**
  - Server logs hold store identifiers, error messages and request paths, not customer data (one remaining log line in EU Compliance is replaced by a hashed reference from 12 Nov 2026).

    - Error alerts mailed to the Manager carry no store domain, e-mail address or long ids; the full context stays in the server log.
    - Server log retention: 7 days (Railway Hobby plan).
- **Availability.** Continuous database replication (Litestream, 1-second interval) or a nightly backup (LUCID, Kündigungsbutton, German Invoices). Services with Litestream refuse to start on an empty database, so that data is not overwritten by mistake.
- **Deletion.**
    - Per clause 9.
    - Price history: 400 days (Shopify) or the configured period (Wix).
    - Login log: 90 days. Access log: 12 months.
    - Backups: 30 days (LUCID 7).
- **Monitoring and incidents.** Automated error and health monitoring with alerts to the Manager around the clock; breach handling per clause 8.
- **Sub-processors.** Selected for their DPA and transfer tools (Annex 3); reviewed on every change notice.

Annex 3 — Sub-processors (SCC Annex III)

Not sub-processors:

- **Shopify and Wix.** These are the Controller's own platforms, under the Controller's own contract with them. Withdrawal acknowledgements of the Wix app go through the Controller's own Wix e-mail service.
- **Stripe.** It processes only the Processor's own billing data. The Kündigungsbutton and German Invoices work in the Controller's own Stripe account, where Stripe is the Controller's own provider under the Controller's own contract.
- **GitHub.** It holds no personal data.

Sub-processor	Address	Purpose / apps	Location of data	Transfer tool	Own sub-processor list / notice period	DPA
Railway Corporation	548 Market St PMB 68956, San Francisco, CA 94104, USA	Hosting of application and database; all apps in Annex 1 except the Wix apps Export für DATEV, BMD-Export, OSS Report and LUCID Report	EU (Amsterdam, europe-west4)	SCCs Module 3 (Railway DPA; Clause 9 Option 1 with 10 days' notice); DPF alternative	https://trust.railway.com/item/subprocessors — 10 days	https://railway.com/legal/dpa
Cloudflare, Inc.	101 Townsend Street, San Francisco, CA 94107, USA	Backup storage (R2) for DATEV/BMD, EU Compliance (Shopify and Wix server), LUCID, buchungsstapel.de, Kündigungsbutton, German Invoices	EU (R2 EU jurisdiction)	SCCs Modules 2/3 (Cloudflare DPA s.6.2); EU-US DPF	https://www.cloudflare.com/gdpr/subprocessors/ — 30 days	https://www.cloudflare.com/cloudflare-customer-dpa/
Plus Five Five, Inc. ("Resend")	2261 Market Street #5039, San Francisco, CA 94114, USA	Sending e-mails: withdrawal and cancellation acknowledgements and notices, invoices and cancellation documents to buyers, accountant links, threshold notices, login links, DATEV files to the account owner, problem reports	Sent from the EU region (Ireland, eu-west-1); stored in the USA	SCCs Modules 2/3 (Resend DPA s.6.2, deemed signed); EU-US DPF (re-certification under review as of Nov 2026)	https://resend.com/legal/subprocessors — 14 days	https://resend.com/legal/dpa
Zoho Corporation GmbH (contracting entity for accounts in Germany; the account's country is Germany)	per https://www.zoho.com/legal/zoho-contracting-entities.html	Support mailbox (support requests and problem reports, which can contain store data)	USA (zoho.com data centre); move to the EU data centre requested 8 Nov 2026	SCCs per Zoho DPA, requested from legal@zohocorp.com on 8 Nov 2026	https://www.zoho.com/privacy/sub-processors.html — no fixed period; change notifications by subscription (treated as short notice, clause 5.3a)	on request (legal@zohocorp.com)

Annex 4 — Standard contractual clauses (Module Two)

This annex applies to the extent that processing by the Processor is a transfer of personal data to a third country (clause 6.1). To that extent, the parties agree the standard contractual clauses under Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), as follows:

- **Information:** taken from Annexes 1–3.
- **Text:** the official text is attached to the PDF of this agreement.
- **Clause 7 (docking clause):** applies.
- **Clause 9(a):** Option 2, general written authorisation, notice as in clause 5.
- **Clause 11(a):** the optional independent dispute resolution body is not used.
- **Clause 13:** the supervisory authority of the data exporter's Member State.
- **Clause 17:** Option 2, the law of the data exporter's Member State; fallback Ireland.
- **Clause 18(b):** the courts of the data exporter's Member State.
- **Conflicts:** where this agreement and the clauses conflict, the clauses prevail.

Where the Processor's processing is itself subject to the GDPR, the Commission considers these clauses not to fit (SCC Q&A); they then apply as a contractual safeguard until the Commission adopts clauses for that case, which the Processor will then offer instead.

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/914 DER KOMMISSION

vom 4. Juni 2021

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

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ([1]), insbesondere auf Artikel 28 Absatz 7 und Artikel 46 Absatz 2 Buchstabe c,

in Erwägung nachstehender Gründe:

(1) Technologische Entwicklungen erleichtern den grenzüberschreitenden Datenverkehr, der für den Ausbau der internationalen Zusammenarbeit und des internationalen Handels erforderlich ist. Gleichzeitig muss bei der Übermittlung personenbezogener Daten an Drittländer, einschließlich im Falle von Weiterübermittlungen, sichergestellt werden, dass das durch die Verordnung (EU) 2016/679 gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird ([2]). Die Bestimmungen über Datenübermittlungen in Kapitel V der Verordnung (EU) 2016/679 sollen den Fortbestand dieses hohen Schutzniveaus bei der Übermittlung personenbezogener Daten an ein Drittland gewährleisten ([3]).

(2) Gemäß Artikel 46 Absatz 1 der Verordnung (EU) 2016/679 darf ein Verantwortlicher oder ein Auftragsverarbeiter — wenn kein Angemessenheitsbeschluss der Kommission nach Artikel 45 Absatz 3 vorliegt — personenbezogene Daten an ein Drittland nur übermitteln, sofern er geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Solche Garantien können in Standarddatenschutzklauseln bestehen, die von der Kommission gemäß Artikel 46 Absatz 2 Buchstabe c erlassen werden.

(3) Die Rolle von Standardvertragsklauseln beschränkt sich auf die Gewährleistung angemessener Datenschutzgarantien für internationale Datenübermittlungen. Daher steht es dem Verantwortlichen oder dem Auftragsverarbeiter, der die personenbezogenen Daten an ein Drittland übermittelt („Datenexporteur"), und dem die personenbezogenen Daten annehmenden Verantwortlichen oder Auftragsverarbeiter („Datenimporteur") frei, diese Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Standardvertragsklauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden. Die Verantwortlichen und die Auftragsverarbeiter werden ermutigt, mittels vertraglicher Verpflichtungen, die die Standardvertragsklauseln ergänzen, zusätzliche Garantien zu bieten ([4]). Der Rückgriff auf die Standardvertragsklauseln erfolgt unbeschadet der vertraglichen Pflichten des Datenexporteurs und/oder des Datenimporteurs, die Einhaltung der geltenden Vorrechte und Befreiungen zu gewährleisten.

(4) Über den Rückgriff auf Standardvertragsklauseln (mit dem Ziel, geeignete Garantien für Datenübermittlungen nach Artikel 46 Absatz 1 der Verordnung (EU) 2016/679 zu bieten) hinaus muss der Datenexporteur seinen allgemeinen Pflichten als Verantwortlicher oder Auftragsverarbeiter gemäß der Verordnung (EU) 2016/679 nachkommen. Diese Pflichten schließen die Pflicht des Verantwortlichen ein, die betroffenen Personen nach Artikel 13 Absatz 1 Buchstabe f und Artikel 14 Absatz 1 Buchstabe f Verordnung (EU) 2016/679 über die beabsichtigte Übermittlung personenbezogener Daten an ein Drittland zu informieren. Im Falle von Datenübermittlungen gemäß Artikel 46 der Verordnung (EU) 2016/679 muss diese Information einen Verweis auf die angemessenen Garantien und die Möglichkeiten, wie eine Kopie von ihnen eingeholt werden kann, oder wo sie verfügbar sind, umfassen.

([1]) ABl. L 119 vom 4.5.2016, S. 1.
([2]) Artikel 44 der Verordnung (EU) 2016/679.
([3]) Siehe auch das Urteil des Gerichtshofs vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems (im Folgenden „Schrems II"), Rechtssache C-311/18, ECLI:EU:C:2020:559, Rn. 93.
([4]) Erwägungsgrund 109 der Verordnung (EU) 2016/679.

(5) Die Entscheidung 2001/497/EG der Kommission ([5]) und der Beschluss 2010/87/EU der Kommission ([6]) enthalten Standardvertragsklauseln, um die Übermittlung personenbezogener Daten von einem in der Union niedergelassenen Verantwortlichen an einen Verantwortlichen oder einen Auftragsverarbeiter zu erleichtern, der in einem Drittland niedergelassen ist, das kein angemessenes Schutzniveau bietet. Diese Entscheidung und dieser Beschluss beruhten auf der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ([7]).

(6) Gemäß Artikel 46 Absatz 5 der Verordnung (EU) 2016/679 bleiben die Entscheidung 2001/497/EG und der Beschluss 2010/87/EU so lange in Kraft, bis sie erforderlichenfalls mit einem nach Artikel 46 Absatz 2 besagter Verordnung erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden. Die Standardvertragsklauseln in dieser Entscheidung bzw. in diesem Beschluss mussten im Lichte der neuen Anforderungen der Verordnung (EU) 2016/679 aktualisiert werden. Darüber hinaus haben sich seit dem Erlass der genannten Entscheidung und des genannten Beschlusses wichtige Entwicklungen in der digitalen Wirtschaft vollzogen, in deren Rahmen neue und komplexere Verarbeitungsvorgänge, an denen häufig mehrere Datenimporteure und Datenexporteure beteiligt sind, lange und komplexe Verarbeitungsketten sowie geänderte Geschäftsbeziehungen allgemein Anwendung finden. Dadurch war eine Modernisierung der Standardvertragsklauseln notwendig, um diese Realitäten besser widerzuspiegeln, indem zusätzliche Verarbeitungs- und Übermittlungsszenarien erfasst werden und ein flexiblerer Ansatz möglich ist, beispielsweise in Bezug auf die Anzahl der Parteien, die dem Vertrag beitreten können.

(7) Unbeschadet der Auslegung des Begriffs der internationalen Datenübermittlung gemäß der Verordnung (EU) 2016/679 können die im Anhang dieses Beschlusses aufgeführten Standardvertragsklauseln von einem Verantwortlichen oder einem Auftragsverarbeiter verwendet werden, um geeignete Garantien im Sinne des Artikels 46 Absatz 1 der Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten an einen in einem Drittland niedergelassenen Auftragsverarbeiter oder Verantwortlichen zu gewährleisten. Die Standardvertragsklauseln dürfen nur insoweit für derartige Datenübermittlungen verwendet werden, als die Verarbeitung durch den Datenimporteur nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt. Dies schließt auch die Übermittlung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter ein, soweit die Verarbeitung Artikel 3 Absatz 2 der Verordnung (EU) 2016/679 unterliegt, da die Datenübermittlung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten oder das Verhalten betroffener Personen zu beobachten, soweit dieses in der Union erfolgt.

(8) Angesichts der allgemeinen Angleichung der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([8]) sollte es möglich sein, die Standardvertragsklauseln auch im Zusammenhang mit einem Vertrag gemäß Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 für die Übermittlung personenbezogener Daten an einen Unterauftragsverarbeiter in einem Drittland durch einen Auftragsverarbeiter zu verwenden, bei dem es sich nicht um ein Organ oder eine Einrichtung der Union handelt, der aber an die Verordnung (EU) 2016/679 gebunden ist und personenbezogene Daten im Auftrag eines Organs oder einer Einrichtung der Union gemäß Artikel 29 der Verordnung (EU) 2018/1725 verarbeitet. Sofern der Vertrag dieselben Datenschutzpflichten widerspiegelt, die im Vertrag oder in einem anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 festgelegt sind, insbesondere indem hinreichende Garantien für technische und organisatorische Maßnahmen geboten werden, die eine Verarbeitung im Einklang mit den Anforderungen dieser Verordnung gewährleisten, wird dadurch die Einhaltung von Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725 sichergestellt. Dies ist insbesondere dann der Fall, wenn sich der Verantwortliche und der Auftragsverarbeiter auf die Standardvertragsklauseln im Durchführungsbeschluss der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([9]) stützen.

(9) Umfasst die Verarbeitung Datenübermittlungen von der Verordnung (EU) 2016/679 unterliegenden Verantwortlichen an Auftragsverarbeiter außerhalb des räumlichen Anwendungsbereichs dieser Verordnung oder von der Verordnung (EU) 2016/679 unterliegenden Auftragsverarbeitern an Unterauftragsverarbeiter außerhalb des räumlichen Anwendungsbereichs dieser Verordnung, so sollten die Standardvertragsklauseln im Anhang dieses Beschlusses auch die Erfüllung der Anforderungen in Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 ermöglichen.

(10) In den im Anhang dieses Beschlusses aufgeführten Standardvertragsklauseln werden allgemeine Klauseln mit einem modularen Ansatz kombiniert, um verschiedenen Datenübermittlungsszenarien und der Komplexität moderner Verarbeitungsketten Rechnung zu tragen. Zusätzlich zu den allgemeinen Klauseln sollten Verantwortliche und Auftragsverarbeiter das für ihre Situation geltende Modul auswählen; auf diese Weise können sie ihre Pflichten

([5]) Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (ABl. L 181 vom 4.7.2001, S. 19).

([6]) Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. L 39 vom 12.2.2010, S. 5).

([7]) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

([8]) 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); siehe Erwägungsgrund 5.

([9]) C(2021) 3701.

gemäß den Standardvertragsklauseln auf ihre jeweilige Rolle und jeweiligen Verantwortlichkeiten hinsichtlich der betreffenden Datenverarbeitung zuschneiden. Mehr als zwei Parteien sollten sich an die Standardvertragsklauseln halten können. Darüber hinaus sollten weitere Verantwortliche und Auftragsverarbeiter den Standardvertragsklauseln während der gesamten Laufzeit des Vertrags, der diese Klauseln als Bestandteile enthält, als Datenexporteure oder Datenimporteure beitreten dürfen.

(11) Um geeignete Garantien zu bieten, sollten die Standardvertragsklauseln gewährleisten, dass für die auf dieser Grundlage übermittelten personenbezogenen Daten ein Schutzniveau besteht, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist ([10]). Um die Transparenz der Verarbeitung zu gewährleisten, sollten die betroffenen Personen eine Kopie der Standardvertragsklauseln erhalten und insbesondere über die Kategorien der verarbeiteten personenbezogenen Daten, das Recht auf Erhalt einer Kopie der Standardvertragsklauseln und jede Weiterübermittlung informiert werden. Weiterübermittlungen durch den Datenimporteur an einen Dritten in einem anderen Drittland sollten nur zulässig sein, wenn dieser Dritte den Standardvertragsklauseln beitritt oder wenn der Fortbestand des Schutzes auf andere Weise gewährleistet ist, oder in bestimmten Situationen, zum Beispiel auf der Grundlage der ausdrücklichen Zustimmung der betroffenen Person nach Inkenntnissetzung.

(12) Von einigen Ausnahmen abgesehen, insbesondere in Bezug auf bestimmte Pflichten, die ausschließlich die Beziehung zwischen dem Datenexporteur und dem Datenimporteur betreffen, sollten betroffene Personen die Standardvertragsklauseln als Drittbegünstigte geltend machen und erforderlichenfalls durchsetzen können. Daher sollten die Parteien zwar die Möglichkeit haben, das Recht eines der Mitgliedstaaten als geltendes Recht für die Standardvertragsklauseln zu wählen, doch müssen in diesem Recht Rechte als Drittbegünstigte zulässig sein. Zur Erleichterung des individuellen Rechtsbehelfs sollte der Datenimporteur durch die Standardvertragsklauseln verpflichtet werden, den betroffenen Personen eine Anlaufstelle mitzuteilen und Beschwerden oder Anträge unverzüglich zu bearbeiten. Bei Streitigkeiten zwischen dem Datenimporteur und einer betroffenen Person, die ihre Rechte als Drittbegünstigte geltend macht, sollte die betroffene Person in der Lage sein, bei der zuständigen Aufsichtsbehörde Beschwerde einzulegen oder die Streitigkeit an die zuständigen Gerichte in der EU zu verweisen.

(13) Um eine wirksame Durchsetzung zu gewährleisten, sollte sich der Datenimporteur der Zuständigkeit der betreffenden Behörde und Gerichte unterwerfen und sich zur Befolgung der verbindlichen Entscheidungen nach dem geltenden Recht des Mitgliedstaats verpflichten müssen. Insbesondere sollte sich der Datenimporteur damit einverstanden erklären, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Darüber hinaus sollte der Datenimporteur die Möglichkeit haben, betroffenen Personen anzubieten, sich an eine unabhängige Streitbeilegungsstelle zu wenden, ohne dass ihnen Kosten entstehen. Im Einklang mit Artikel 80 Absatz 1 der Verordnung (EU) 2016/679 sollte es betroffenen Personen gestattet sein, sich bei Streitigkeiten mit dem Datenimporteur durch Vereinigungen oder andere Einrichtungen vertreten zu lassen, wenn sie dies wünschen.

(14) Die Standardvertragsklauseln sollten Vorschriften über die Haftung zwischen den Parteien und in Bezug auf betroffene Personen sowie Entschädigungsregelungen zwischen den Parteien vorsehen. Wenn der betroffenen Person infolge einer Verletzung der ihr nach den Standardvertragsklauseln zugestandenen Rechte als Drittbegünstigte ein materieller oder immaterieller Schaden entsteht, sollte sie Anspruch auf Entschädigung haben. Eine etwaige Haftung gemäß der Verordnung (EU) 2016/679 sollte davon unberührt bleiben.

(15) Im Falle einer Datenübermittlung an einen Datenimporteur, der als Auftragsverarbeiter oder Unterauftragsverarbeiter fungiert, sollten gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 spezielle Anforderungen gelten. In den Standardvertragsklauseln sollte vorgesehen werden, den Datenimporteur dazu zu verpflichten, alle erforderlichen Informationen zum Nachweis der Einhaltung der in den Klauseln festgelegten Pflichten zur Verfügung zu stellen und dem Datenexporteur die Prüfung seiner Verarbeitungstätigkeiten zu ermöglichen und zu einer solchen Prüfung beizutragen. Im Hinblick auf die Beauftragung eines Unterauftragsverarbeiters durch den Datenimporteur gemäß Artikel 28 Absätze 2 und 4 der Verordnung (EU) 2016/679 sollten in den Standardvertragsklauseln speziell das Verfahren für die allgemeine oder gesonderte Genehmigung seitens des Datenexporteurs sowie die Anforderung festgelegt werden, dass ein schriftlicher Vertrag mit dem Unterauftragsverarbeiter zu schließen ist, der das gleiche Schutzniveau wie die Klauseln gewährleistet.

(16) Es ist angebracht, in den Standardvertragsklauseln unterschiedliche Garantien vorzusehen, die den spezifischen Fall abdecken, dass ein in der Union ansässiger Auftragsverarbeiter personenbezogene Daten an seinen in einem Drittland ansässigen Verantwortlichen übermittelt, und die die begrenzten eigenständigen Pflichten der Auftragsverarbeiter gemäß der Verordnung (EU) 2016/679 widerspiegeln. Insbesondere sollte der Auftragsverarbeiter gemäß den Standardvertragsklauseln verpflichtet sein, den Verantwortlichen zu informieren, wenn er dessen Anweisungen nicht befolgen kann, einschließlich in dem Fall, wenn diese Anweisungen gegen das Datenschutzrecht der Union verstoßen; außerdem sollten die Standardvertragsklauseln den Verantwortlichen verpflichten, alle Handlungen zu unterlassen, die den Auftragsverarbeiter daran hindern würden, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen. Ferner sollten die Parteien durch die Klauseln verpflichtet werden, sich gegenseitig bei der Beantwortung von Anfragen und Anträgen zu unterstützen, die von betroffenen Personen gemäß den für den Datenimporteur geltenden lokalen Rechtsvorschriften oder — bei der Datenverarbeitung in der Union — gemäß der

([10]) Schrems II, Rn. 96 und 103. Siehe auch Verordnung (EU) 2016/679, Erwägungsgründe 108 und 114.

Verordnung (EU) 2016/679 gestellt werden. Zusätzliche Anforderungen sollten gelten, um etwaige Auswirkungen der Rechtsvorschriften des Bestimmungsdrittlandes auf die Einhaltung der Klauseln durch den Verantwortlichen zu berücksichtigen, insbesondere in Bezug auf den Umgang mit bindenden Ersuchen von Behörden im Drittland um Offenlegung der übermittelten personenbezogenen Daten, wenn der in der Union ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der Union erhoben wurden. Dagegen sind solche Anforderungen nicht gerechtfertigt, wenn die Auslagerung lediglich die Verarbeitung und die Rückübertragung der vom Verantwortlichen erhaltenen personenbezogener Daten umfasst und der Verantwortliche in jedem Fall der Gerichtsbarkeit des betreffenden Drittlandes unterliegt und weiterhin unterliegen wird.

(17) Die Parteien sollten in der Lage sein, die Einhaltung der Standardvertragsklauseln nachzuweisen. Insbesondere sollte der Datenimporteur verpflichtet sein, geeignete Nachweise für die unter seiner Verantwortung durchgeführten Verarbeitungstätigkeiten aufzubewahren und den Datenexporteur unverzüglich in Kenntnis zu setzen, wenn er aus welchen Gründen auch immer nicht in der Lage ist, die Klauseln einzuhalten. Der Datenexporteur sollte seinerseits die Datenübermittlung aussetzen und in besonders schweren Fällen das Recht haben, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß Standardvertragsklauseln geht, wenn der Datenimporteur gegen die Standardvertragsklauseln verstößt oder diese nicht einhalten kann. Wenn sich lokale Rechtsvorschriften auf die Einhaltung der Klauseln auswirken, sollten besondere Vorschriften gelten. Personenbezogene Daten, die vor Beendigung des Vertrags übermittelt wurden, sowie Kopien davon sollten nach Wahl des Datenexporteurs an diesen zurückgegeben oder vollständig vernichtet werden.

(18) Die Standardvertragsklauseln sollten — insbesondere im Lichte der Rechtsprechung des Gerichtshofs ([11]) — spezifische Garantien vorsehen, um etwaige Auswirkungen der Rechtsvorschriften des Bestimmungsdrittlandes auf die Einhaltung der Klauseln durch den Datenimporteur zu berücksichtigen, speziell in Bezug auf den Umgang mit bindenden Ersuchen von Behörden in diesem Land um Offenlegung der übermittelten personenbezogenen Daten.

(19) Die Übermittlung und Verarbeitung personenbezogener Daten im Rahmen von Standardvertragsklauseln sollten nicht erfolgen, wenn die Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes den Datenimporteur an der Einhaltung der Klauseln hindern. In diesem Zusammenhang sollten 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 als im Widerspruch zu den Standardvertragsklauseln stehend betrachtet werden. Die Parteien sollten zusichern, dass sie zum Zeitpunkt der Zustimmung zu den Standardvertragsklauseln keinen Grund zu der Annahme haben, dass die für den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten diesen Anforderungen nicht entsprechen.

(20) Die Partien sollten insbesondere den besonderen Umständen der Übermittlung (wie Inhalt und Dauer des Vertrags, Art der zu übermittelnden Daten, Art des Empfängers, Zweck der Verarbeitung), den Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes, die angesichts der Umstände der Übermittlung relevant sind, und etwaigen Garantien zur Ergänzung der Garantien gemäß den Standardvertragsklauseln (einschließlich der einschlägigen vertraglichen, technischen und organisatorischen Maßnahmen, die für die Übermittlung und die Verarbeitung der personenbezogenen Daten im Bestimmungsland gelten) Rechnung tragen. Was die Auswirkungen solcher Rechtsvorschriften und Gepflogenheiten auf die Einhaltung der Standardvertragsklauseln betrifft, so können im Rahmen einer Gesamtbeurteilung verschiedene Aspekte betrachtet werden, darunter zuverlässige Informationen über die Anwendung der Rechtsvorschriften in der Praxis (z. B. Rechtsprechung und Berichte unabhängiger Aufsichtsgremien), das Vorliegen oder Nichtvorliegen von Anträgen innerhalb desselben Sektors und, unter strengen Voraussetzungen, die dokumentierte praktische Erfahrung des Datenexporteurs und Datenimporteurs.

(21) Der Datenimporteur sollte den Datenexporteur darüber informieren, wenn er nach Zustimmung zu den Standardvertragsklauseln Grund zu der Annahme hat, dass er nicht in der Lage ist, die Standardvertragsklauseln einzuhalten. Erhält der Datenexporteur eine solche Mitteilung oder erhält er auf andere Weise Kenntnis davon, dass der Datenimporteur nicht mehr in der Lage ist, die Standardvertragsklauseln einzuhalten, sollte er geeignete Abhilfemaßnahmen ermitteln, erforderlichenfalls in Abstimmung mit der zuständigen Aufsichtsbehörde. Diese Maßnahmen können ergänzende Maßnahmen des Datenexporteurs und/oder des Datenimporteurs umfassen, zum Beispiel technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit. Der Datenexporteur sollte verpflichtet werden, die Datenübermittlung auszusetzen, wenn er der Auffassung ist, dass keine angemessenen Garantien gewährleistet werden können, oder wenn er von der zuständigen Aufsichtsbehörde dazu angewiesen wird.

([11]) Schrems II.

(22) Soweit möglich, sollte der Datenimporteur den Datenexporteur und die betroffene Person benachrichtigen, wenn er von einer Behörde (auch einer Justizbehörde) ein nach dem Recht des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß den Standardvertragsklauseln übermittelt wurden. Gleichermaßen sollte der Datenimporteur den Datenexporteur und die betroffene Person benachrichtigen, wenn er davon Kenntnis erhält, dass eine Behörde nach dem Recht des Bestimmungsdrittlandes direkten Zugang zu diesen personenbezogenen Daten hat. Ist der Datenimporteur trotz aller Anstrengungen nicht in der Lage, den Datenexporteur und/oder die betroffene Person über spezifische Offenlegungsersuchen zu informieren, sollte er dem Datenexporteur möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung stellen. Darüber hinaus sollte der Datenimporteur dem Datenexporteur in regelmäßigen Abständen aggregierte Informationen bereitstellen. Der Datenimporteur sollte außerdem verpflichtet sein, alle eingegangenen Offenlegungsersuchen und die übermittelten Antworten zu dokumentieren und diese Informationen dem Datenexporteur oder der zuständigen Aufsichtsbehörde oder beiden auf Verlangen zur Verfügung zu stellen. Kommt der Datenimporteur nach einer Prüfung der Rechtmäßigkeit eines solchen Ersuchens nach den Rechtsvorschriften des Bestimmungslandes zu dem Schluss, dass hinreichende Gründe für die Annahme bestehen, dass der Antrag nach den Rechtsvorschriften des Bestimmungsdrittlandes rechtswidrig ist, sollte er das Ersuchen anfechten und gegebenenfalls die verfügbaren Rechtsmittel ausschöpfen. Ist der Datenimporteur nicht mehr in der Lage, die Standardvertragsklauseln einzuhalten, sollte er den Datenexporteur in jedem Fall entsprechend informieren, auch dann, wenn dies die Folge eines Offenlegungsersuchens ist.

(23) Da sich die Bedürfnisse der Interessenträger, die Technologie und die Verarbeitungsvorgänge ändern können, sollte die Kommission im Rahmen der nach Artikel 97 der Verordnung (EU) 2016/679 erforderlichen regelmäßigen Bewertung dieser Verordnung die Funktion der Standardvertragsklauseln vor dem Hintergrund der gesammelten Erfahrungen prüfen.

(24) Die Entscheidung 2001/497/EG und der Beschluss 2010/87/EU sollten drei Monate nach Inkrafttreten des vorliegenden Beschlusses aufgehoben werden. Allerdings sollten die Datenexporteure und Datenimporteure innerhalb dieses Zeitraums die Standardvertragsklauseln der Entscheidung 2001/497/EG und des Beschlusses 2010/87/EU für die Zwecke des Artikels 46 Absatz 1 der Verordnung (EU) 2016/679 weiterhin verwenden können. Für einen weiteren Zeitraum von 15 Monaten sollten sich Datenexporteure und Datenimporteure für die Zwecke des Artikels 46 Absatz 1 der Verordnung (EU) 2016/679 weiterhin auf die Standardvertragsklauseln der Entscheidung 2001/497/EG und des Beschlusses 2010/87/EU stützen können, um vor dem Datum der Aufhebung dieser Entscheidung und dieses Beschlusses zwischen ihnen geschlossene Verträge zu erfüllen, sofern die Verarbeitungsvorgänge, die Gegenstand des Vertrags sind, unverändert bleiben und die Anwendung der Klauseln gewährleistet, dass die Übermittlung personenbezogener Daten geeigneten Garantien im Sinne des Artikels 46 Absatz 1 der Verordnung (EU) 2016/679 unterliegt. Im Falle relevanter Vertragsänderungen sollte der Datenexporteur verpflichtet sein, sich auf einen neuen Grund für Datenübermittlungen im Rahmen des Vertrags zu stützen, insbesondere indem er die bestehenden Standardvertragsklauseln durch die im Anhang des vorliegenden Beschlusses aufgeführten Standardvertragsklauseln ersetzt. Gleiches sollte für jede Unterauftragsvergabe von Verarbeitungsvorgängen, die Gegenstand des Vertrags sind, an einen (Unter-)Auftragsverarbeiter gelten.

(25) Gemäß Artikel 42 Absätze 1 und 2 der Verordnung (EU) 2018/1725 wurden der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss konsultiert; diese haben am 14. Januar 2021 eine gemeinsame Stellungnahme ([12]) abgegeben, die bei der Ausarbeitung des vorliegenden Beschlusses berücksichtigt wurde.

(26) Die in diesem Beschluss vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des gemäß Artikel 93 der Verordnung (EU) 2016/679 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Die im Anhang aufgeführten Standardvertragsklauseln gelten als geeignete Garantien im Sinne des Artikels 46 Absatz 1 und des Artikels 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 für die Übermittlung von gemäß dieser Verordnung verarbeiteten personenbezogenen Daten durch einen Verantwortlichen oder einen Auftragsverarbeiter (Datenexporteur) an einen Verantwortlichen oder einen (Unter-)Auftragsverarbeiter, dessen Verarbeitung der Daten nicht dieser Verordnung unterliegt (Datenimporteur).

(2) In den Standardvertragsklauseln sind auch die Rechte und Pflichten der Verantwortlichen und der Auftragsverarbeiter in Bezug auf die in Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 genannten Fragen im Hinblick auf die Übermittlung personenbezogener Daten von einem Verantwortlichen an einen Auftragsverarbeiter oder von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter festgelegt.

([12]) Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer für die in Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 genannten Angelegenheiten.

Artikel 2

Wenn die zuständigen Behörden der Mitgliedstaaten ihre Abhilfebefugnisse gemäß Artikel 58 der Verordnung (EU) 2016/679 ausüben, weil in den Rechtsvorschriften oder in der Praxis des Bestimmungsdrittlands Bestimmungen gelten oder gelten werden, die den Datenimporteur daran hindern, die im Anhang aufgeführten Standardvertragsklauseln einzuhalten — was zur Aussetzung oder Untersagung von Datenübermittlungen an Drittländer führt —, so unterrichtet der betreffende Mitgliedstaat unverzüglich die Kommission, die die Informationen an die anderen Mitgliedstaaten weiterleitet.

Artikel 3

Die Kommission prüft die praktische Anwendung der im Anhang aufgeführten Standardvertragsklauseln auf der Grundlage aller verfügbaren Informationen im Rahmen der gemäß Artikel 97 der Verordnung (EU) 2016/679 erforderlichen regelmäßigen Bewertung.

Artikel 4

(1) Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Die Entscheidung 2001/497/EG wird mit Wirkung vom 27. September 2021 aufgehoben.

(3) Der Beschluss 2010/87/EU wird mit Wirkung vom 27. September 2021 aufgehoben.

(4) In Bezug auf Verträge, die vor dem 27. September 2021 auf Grundlage der Entscheidung 2001/497/EG oder des Beschlusses 2010/87/EU geschlossen wurden, wird davon ausgegangen, dass sie geeignete Garantien im Sinne des Artikels 46 Absatz 1 der Verordnung (EU) 2016/679 bis zum 27. Dezember 2022 bieten, sofern die Verarbeitungsvorgänge, die Gegenstand des Vertrags sind, unverändert bleiben und die Anwendung dieser Klauseln gewährleistet, dass die Übermittlung personenbezogener Daten geeigneten Garantien unterliegt.

Brüssel, den 4. Juni 2021

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

STANDARDVERTRAGSKLAUSELN

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:

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

([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.

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

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung der Parteien jederzeit entweder als Datenexporteur oder als Datenimporteur beitreten, indem sie die Anlage ausfüllt und Anhang I.A unterzeichnet.

b) Nach Ausfüllen der Anlage und Unterzeichnung von Anhang I.A wird die beitretende Einrichtung Partei dieser Klauseln und hat die Rechte und Pflichten eines Datenexporteurs oder eines Datenimporteurs entsprechend ihrer Bezeichnung in Anhang I.A.

c) Für den Zeitraum vor ihrem Beitritt als Partei erwachsen der beitretenden Einrichtung keine Rechte oder Pflichten aus diesen Klauseln.

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

8.1. **Zweckbindung**

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Zweck(e) der Übermittlung. Er darf die personenbezogenen Daten nur dann für einen anderen Zweck verarbeiten,

i) wenn er die vorherige Einwilligung der betroffenen Person eingeholt hat,

ii) wenn dies zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder

iii) wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist.

8.2. **Transparenz**

a) Damit betroffene Personen ihre Rechte gemäß Klausel 10 wirksam ausüben können, teilt der Datenimporteur ihnen entweder direkt oder über den Datenexporteur Folgendes mit:

i) seinen Namen und seine Kontaktdaten,

ii) die Kategorien der verarbeiteten personenbezogenen Daten,

iii) das Recht auf Erhalt einer Kopie dieser Klauseln,

iv) wenn er eine Weiterübermittlung der personenbezogenen Daten an Dritte beabsichtigt, den Empfänger oder die Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), den Zweck und den Grund einer solchen Weiterübermittlung gemäß Klausel 8.7.

b) Buchstabe a findet keine Anwendung, wenn die betroffene Person bereits über die Informationen verfügt, einschließlich in dem Fall, wenn diese Informationen bereits vom Datenexporteur bereitgestellt wurden, oder wenn sich die Bereitstellung der Informationen als nicht möglich erweist oder einen unverhältnismäßigen Aufwand für den Datenimporteur mit sich bringen würde. Im letzteren Fall macht der Datenimporteur die Informationen, soweit möglich, öffentlich zugänglich.

c) Die Parteien stellen der betroffenen Person auf Anfrage eine Kopie dieser Klauseln, einschließlich der von ihnen ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, können die Parteien Teile des Textes der Anlage vor der Weitergabe einer Kopie unkenntlich machen; sie legen 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.

d) Die Buchstaben a bis c gelten unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.3. **Richtigkeit und Datenminimierung**

a) Jede Partei stellt sicher, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind. Der Datenimporteur trifft alle angemessenen Maßnahmen, um sicherzustellen, dass personenbezogene Daten, die im Hinblick auf den/die Zweck(e) der Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

b) Stellt eine der Parteien fest, dass die von ihr übermittelten oder erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet sie unverzüglich die andere Partei.

c) Der Datenimporteur stellt sicher, dass die personenbezogenen Daten angemessen und erheblich sowie auf das für den/die Zweck(e) ihrer Verarbeitung notwendige Maß beschränkt sind.

8.4. **Speicherbegrenzung**

Der Datenimporteur speichert die personenbezogenen Daten nur so lange, wie es für den/die Zweck(e), für den/die sie verarbeitet werden, erforderlich ist. Er trifft geeignete technische oder organisatorische Maßnahmen, um die Einhaltung dieser Verpflichtung sicherzustellen; hierzu zählen auch die Löschung oder Anonymisierung ([2]) der Daten und aller Sicherungskopien am Ende der Speicherfrist.

8.5. **Sicherheit der Verarbeitung**

a) Der Datenimporteur und — während der Datenübermittlung — auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen 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 den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie 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 betroffene Person gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

b) Die Parteien haben sich auf die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen geeinigt. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

c) Der Datenimporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

d) 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 des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

e) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, meldet der Datenimporteur die Verletzung unverzüglich sowohl dem Datenexporteur als auch der gemäß Klausel 13 festgelegten zuständigen Aufsichtsbehörde. Diese Meldung enthält i) 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), ii) ihre wahrscheinlichen Folgen, iii) die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und iv) die Kontaktdaten einer Anlaufstelle, bei der weitere Informationen eingeholt werden können. Soweit es dem Datenimporteur nicht möglich ist, alle Informationen zur gleichen Zeit bereitzustellen, kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

f) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Datenimporteur ebenfalls die jeweiligen betroffenen Personen unverzüglich von der Verletzung des Schutzes personenbezogener Daten und der Art der Verletzung, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur, unter Angabe der unter Buchstabe e Ziffern ii bis iv genannten Informationen, es sei denn, der Datenimporteur hat Maßnahmen ergriffen, um das Risiko für die Rechte oder Freiheiten natürlicher Personen erheblich zu mindern, oder die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. Im letzteren Fall gibt der Datenimporteur stattdessen eine öffentliche Bekanntmachung heraus oder ergreift eine vergleichbare Maßnahme, um die Öffentlichkeit über die Verletzung des Schutzes personenbezogener Daten zu informieren.

g) Der Datenimporteur dokumentiert alle maßgeblichen Fakten im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, einschließlich ihrer Auswirkungen und etwaiger ergriffener Abhilfemaßnahmen, und führt Aufzeichnungen darüber.

8.6. **Sensible Daten**

Sofern 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 oder Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Datenimporteur spezielle Beschränkungen und/oder zusätzliche Garantien an, die an die spezifische Art der Daten und die damit verbundenen Risiken angepasst sind. Dies kann die Beschränkung des Personals, das Zugriff auf die personenbezogenen Daten hat, zusätzliche Sicherheitsmaßnahmen (wie Pseudonymisierung) und/oder zusätzliche Beschränkungen in Bezug auf die weitere Offenlegung umfassen.

([2]) Die Daten müssen in einer Weise anonymisiert werden, dass eine Person im Einklang mit Erwägungsgrund 26 der Verordnung (EU) 2016/679 nicht mehr identifizierbar ist; außerdem muss dieser Vorgang unumkehrbar sein.

8.7. **Weiterübermittlungen**

Der Datenimporteur darf die personenbezogenen Daten nicht an Dritte weitergeben, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union ([3]) ansässig sind (im Folgenden „Weiterübermittlung"), es sei denn, der Dritte ist im Rahmen des betreffenden Moduls an diese Klauseln gebunden oder erklärt sich mit der Bindung daran einverstanden. Andernfalls ist eine Weiterübermittlung durch den Datenimporteur nur in folgenden Fällen zulässig:

i) Sie erfolgt an ein Land, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,

ii) der Dritte gewährleistet auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 im Hinblick auf die betreffende Verarbeitung,

iii) der Dritte geht mit dem Datenimporteur ein bindendes Instrument ein, mit dem das gleiche Datenschutzniveau wie gemäß diesen Klauseln gewährleistet wird, und der Datenimporteur stellt dem Datenexporteur eine Kopie dieser Garantien zur Verfügung,

iv) die Weiterübermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich,

v) die Weiterübermittlung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, oder

vi) – falls keine der anderen Bedingungen erfüllt ist — der Datenimporteur hat die ausdrückliche Einwilligung der betroffenen Person zu einer Weiterübermittlung in einem speziellen Fall eingeholt, nachdem er sie über den/die Zweck(e), die Identität des Empfängers und die ihr mangels geeigneter Datenschutzgarantien aus einer solchen Übermittlung möglicherweise erwachsenden Risiken informiert hat. In diesem Fall unterrichtet der Datenimporteur den Datenexporteur und übermittelt ihm auf dessen Verlangen eine Kopie der Informationen, die der betroffenen Person bereitgestellt wurden.

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

8.8. **Verarbeitung unter der Aufsicht des Datenimporteurs**

Der Datenimporteur stellt sicher, dass jede ihm unterstellte Person, einschließlich eines Auftragsverarbeiters, diese Daten ausschließlich auf der Grundlage seiner Weisungen verarbeitet.

8.9. **Dokumentation und Einhaltung der Klauseln**

a) Jede Partei muss nachweisen können, dass sie ihre Pflichten gemäß diesen Klauseln erfüllt. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die unter seiner Verantwortung durchgeführten Verarbeitungstätigkeiten.

b) Der Datenimporteur stellt der zuständigen Aufsichtsbehörde diese Aufzeichnungen auf Verlangen zur Verfügung.

MODUL ZWEI: 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 Anhang I.B genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

([3]) 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.

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 seinen 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 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 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 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 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.

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

8.1. **Weisungen**

a) Der Datenexporteur hat dem Datenimporteur mitgeteilt, dass er als Auftragsverarbeiter nach den Weisungen seines/seiner Verantwortlichen fungiert, und der Datenexporteur stellt dem Datenimporteur diese Weisungen vor der Verarbeitung zur Verfügung.

b) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, sowie auf der Grundlage aller zusätzlichen dokumentierten Weisungen des Datenexporteurs. Diese zusätzlichen Weisungen dürfen nicht im Widerspruch zu den Weisungen des Verantwortlichen stehen. Der Verantwortliche oder der Datenexporteur kann während der gesamten Vertragslaufzeit weitere dokumentierte Weisungen im Hinblick auf die Datenverarbeitung erteilen.

c) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann. Ist der Datenimporteur nicht in der Lage, die Weisungen des Verantwortlichen zu befolgen, setzt der Datenexporteur den Verantwortlichen unverzüglich davon in Kenntnis.

d) Der Datenexporteur sichert zu, dass er dem Datenimporteur dieselben Datenschutzpflichten auferlegt hat, die im Vertrag oder in einem anderen Rechtsinstrument nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zwischen dem Verantwortlichen und dem Datenexporteur festgelegt sind. ([5])

8.2. **Zweckbindung**

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang I.B genannten spezifischen Übermittlungszweck(e), sofern keine weiteren Weisungen seitens des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, oder seitens 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 personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage 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.

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 berichtigen oder zu löschen.

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 Datenverarbeitungsdienste alle im Auftrag des Verantwortlichen 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.

([5]) Siehe Artikel 28 Absatz 4 der Verordnung (EU) 2016/679 und, wenn es sich bei dem Verantwortlichen um ein Organ oder eine Einrichtung der Union handelt, Artikel 29 Absatz 4 der Verordnung (EU) 2018/1725.

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 sie 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 betroffene Person 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 oder des Verantwortlichen. Zur Erfüllung seinen 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 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. Außerdem meldet der Datenimporteur die Verletzung dem Datenexporteur und, sofern angemessen und machbar, dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung 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 des Schutzes der Daten, einschließlich 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 den Verantwortlichen zu unterrichten, damit dieser wiederum die zuständige Aufsichtsbehörde und die betroffenen Personen benachrichtigen kann.

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 Anhang I.B angegebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8. **Weiterübermittlungen**

Der Datenimporteur gibt die personenbezogenen Daten nur auf der Grundlage dokumentierter Weisungen des Verantwortlichen, die dem Datenimporteur vom Datenexporteur mitgeteilt wurden, 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 ([6]) 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,

([6]) 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.

ii) der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung (EU) 2016/679 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 oder des Verantwortlichen, 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 Verantwortlichen durchgeführten Verarbeitungstätigkeiten.

c) Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten Pflichten erforderlich sind, und der Datenexporteur stellt diese Informationen wiederum dem Verantwortlichen bereit.

d) Der Datenimporteur ermöglicht dem Datenexporteur die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Gleiches gilt, wenn der Datenexporteur eine Prüfung auf Weisung des Verantwortlichen beantragt. Bei der Entscheidung über eine Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.

e) Wird die Prüfung auf Weisung des Verantwortlichen durchgeführt, stellt der Datenexporteur die Ergebnisse dem Verantwortlichen zur Verfügung.

f) 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.

g) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben b und c genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

8.1. **Weisungen**

a) Der Datenexporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenimporteurs, der als sein Verantwortlicher fungiert.

b) Der Datenexporteur unterrichtet den Datenimporteur unverzüglich, wenn er die betreffenden Weisungen nicht befolgen kann, u. a. wenn eine solche Weisung gegen die Verordnung (EU) 2016/679 oder andere Datenschutzvorschriften der Union oder eines Mitgliedstaats verstößt.

c) Der Datenimporteur sieht von jeglicher Handlung ab, die den Datenexporteur an der Erfüllung seiner Pflichten gemäß der Verordnung (EU) 2016/679 hindern würde, einschließlich im Zusammenhang mit Unterverarbeitungen oder der Zusammenarbeit mit den zuständigen Aufsichtsbehörden.

d) Nach Wahl des Datenimporteurs löscht der Datenexporteur nach Beendigung der Datenverarbeitungsdienste alle im Auftrag des Datenimporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenimporteur, dass dies erfolgt ist, oder gibt dem Datenimporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien.

8.2. **Sicherheit der Verarbeitung**

a) Die Parteien treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der personenbezogenen Daten, auch während der Übermittlung, sowie den Schutz vor einer Verletzung der Sicherheit zu gewährleisten, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den personenbezogenen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen sie dem Stand der Technik, den Implementierungskosten, der Art der personenbezogenen Daten ([7]), 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 und ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Übermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann.

b) Der Datenexporteur unterstützt den Datenimporteur bei der Gewährleistung einer angemessenen Sicherheit der Daten gemäß Buchstabe a. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Datenexporteur gemäß diesen Klauseln verarbeiteten personenbezogenen Daten meldet der Datenexporteur dem Datenimporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde, und unterstützt den Datenimporteur bei der Behebung der Verletzung.

c) Der Datenexporteur gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.3. **Dokumentation und Einhaltung der Klauseln**

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Datenexporteur stellt dem Datenimporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung seiner Pflichten gemäß diesen Klauseln erforderlich sind, und ermöglicht Prüfungen und trägt zu diesen bei.

Klausel 9

Einsatz von Unterauftragsverarbeitern

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

a) OPTION 1: VORHERIGE GESONDERTE GENEHMIGUNG. Der Datenimporteur darf keine seiner Verarbeitungstätigkeiten, die er im Auftrag des Datenexporteurs gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Datenexporteurs an einen Unterauftragsverarbeiter untervergeben. Der Datenimporteur reicht den Antrag auf die gesonderte Genehmigung mindestens [Zeitraum angeben] vor der Beauftragung des Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Datenexporteur benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Datenexporteur bereits genehmigten Unterauftragsverarbeiter findet sich in Anhang III. Die Parteien halten Anhang III jeweils auf dem neuesten Stand.

OPTION 2: ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG. 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 [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.

([7]) Hierzu zählt, ob die Übermittlung und Weiterverarbeitung personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder 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 oder Straftaten enthalten.

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

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.

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

a) OPTION 1: VORHERIGE GESONDERTE GENEHMIGUNG. Der Datenimporteur darf keine seiner Verarbeitungstätigkeiten, die er im Auftrag des Datenexporteurs gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Datenimporteur reicht den Antrag auf die gesonderte Genehmigung mindestens [*Zeitraum angeben*] vor der Beauftragung des Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Er informiert den Datenexporteur über eine solche Beauftragung. Die Liste der vom Verantwortlichen bereits genehmigten Unterauftragsverarbeiter findet sich in Anhang III. Die Parteien halten Anhang III jeweils auf dem neuesten Stand.

OPTION 2: 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 Verantwortlichen mindestens [*Zeitraum angeben*] im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Der Datenimporteur unterrichtet den Datenexporteur über die Beauftragung des/der Unterauftragsverarbeiter/s.

b) Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), 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. ([9]) 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) Auf Verlangen des Datenexporteurs oder des Verantwortlichen stellt der Datenimporteur 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.

([9]) 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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

a) Der Datenimporteur bearbeitet, gegebenenfalls mit Unterstützung des Datenexporteurs, alle Anfragen und Anträge einer betroffenen Person im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte gemäß diesen Klauseln unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang der Anfrage oder des Antrags. ([10]) Der Datenimporteur trifft geeignete Maßnahmen, um solche Anfragen und Anträge und die Ausübung der Rechte betroffener Personen zu erleichtern. Alle Informationen, die der betroffenen Person zur Verfügung gestellt werden, müssen in verständlicher und leicht zugänglicher Form vorliegen und in einer klaren und einfachen Sprache abgefasst sein.

b) Insbesondere unternimmt der Datenimporteur auf Antrag der betroffenen Person folgende Handlungen, wobei der betroffenen Person keine Kosten entstehen:

   i) Er legt der betroffenen Person eine Bestätigung darüber vor, ob sie betreffende personenbezogene Daten verarbeitet werden, und, falls dies der Fall ist, stellt er ihr eine Kopie der sie betreffenden Daten und die in Anhang I enthaltenen Informationen zur Verfügung; er stellt, falls personenbezogene Daten weiterübermittelt wurden oder werden, Informationen über die Empfänger oder Kategorien von Empfängern (je nach Bedarf zur Bereitstellung aussagekräftiger Informationen), an die die personenbezogenen Daten weiterübermittelt wurden oder werden, sowie über den Zweck dieser Weiterübermittlung und deren Grund gemäß Klausel 8.7 bereit; er informiert die betroffene Person über ihr Recht, gemäß Klausel 12 Buchstabe c Ziffer i bei einer Aufsichtsbehörde Beschwerde einzulegen;

   ii) er berichtigt unrichtige oder unvollständige Daten über die betroffene Person;

   iii) er löscht personenbezogene Daten, die sich auf die betroffene Person beziehen, wenn diese Daten unter Verstoß gegen eine dieser Klauseln, die Rechte als Drittbegünstigte gewährleisten, verarbeitet werden oder wurden oder wenn die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung stützt, widerruft.

c) Verarbeitet der Datenimporteur die personenbezogenen Daten für Zwecke der Direktwerbung, so stellt er die Verarbeitung für diese Zwecke ein, wenn die betroffene Person Widerspruch dagegen einlegt.

d) Der Datenimporteur trifft keine Entscheidung, die ausschließlich auf der automatisierten Verarbeitung der übermittelten personenbezogenen Daten beruht (im Folgenden „automatisierte Entscheidung"), welche rechtliche Wirkung für die betroffene Person entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen würde, es sei denn, die betroffene Person hat hierzu ihre ausdrückliche Einwilligung gegeben oder eine solche Verarbeitung ist nach den Rechtsvorschriften des Bestimmungslandes zulässig und in diesen sind angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person festgelegt. In diesem Fall muss der Datenimporteur, erforderlichenfalls in Zusammenarbeit mit dem Datenexporteur,

   i) die betroffene Person über die geplante automatisierte Entscheidung, die angestrebten Auswirkungen und die damit verbundene Logik unterrichten und

   ii) geeignete Garantien umsetzen, die mindestens bewirken, dass die betroffene Person die Entscheidung anfechten, ihren Standpunkt darlegen und eine Überprüfung durch einen Menschen erwirken kann.

e) Bei exzessiven Anträgen einer betroffenen Person — insbesondere im Fall von häufiger Wiederholung — kann der Datenimporteur entweder eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten für die Erledigung des Antrags verlangen oder sich weigern, aufgrund des Antrags tätig zu werden.

f) Der Datenimporteur kann den Antrag einer betroffenen Person ablehnen, wenn eine solche Ablehnung nach den Rechtsvorschriften des Bestimmungslandes zulässig und in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um eines der in Artikel 23 Absatz 1 der Verordnung (EU) 2016/679 aufgeführten Ziele zu schützen.

g) Beabsichtigt der Datenimporteur, den Antrag einer betroffenen Person abzulehnen, so unterrichtet er die betroffene Person über die Gründe für die Ablehnung und über die Möglichkeit, Beschwerde bei der zuständigen Aufsichtsbehörde einzulegen und/oder einen gerichtlichen Rechtsbehelf einzulegen.

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

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.

([10]) Diese Frist kann um höchstens zwei weitere Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Datenimporteur unterrichtet die betroffene Person ordnungsgemäß und unverzüglich über eine solche Verlängerung.

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 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.

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

a) Der Datenimporteur unterrichtet den Datenexporteur und gegebenenfalls den Verantwortlichen unverzüglich über jeden Antrag, den er von einer betroffenen Person erhält; er beantwortet diesen Antrag erst dann, wenn er vom Verantwortlichen dazu ermächtigt wurde.

b) Der Datenimporteur unterstützt den Verantwortlichen, gegebenenfalls in Zusammenarbeit mit dem Datenexporteur, bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 zu beantworten. Zu diesem Zweck legen die Parteien in 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 Verantwortlichen, die ihm vom Datenexporteur übermittelt wurden.

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Die Parteien unterstützen sich gegenseitig bei der Beantwortung von Anfragen und Anträgen, die von betroffenen Personen gemäß den für den Datenimporteur geltenden lokalen Rechtsvorschriften oder — bei der Datenverarbeitung durch den Datenexporteur in der Union — gemäß der Verordnung (EU) 2016/679 gestellt werden.

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.

[OPTION: Der Datenimporteur erklärt sich damit einverstanden, dass betroffene Personen eine Beschwerde auch bei einer unabhängigen Streitbeilegungsstelle ([11]) einreichen können, ohne dass für die betroffene Person Kosten entstehen. Er unterrichtet die betroffenen Personen in der unter Buchstabe a beschriebenen Weise über einen solchen Rechtsbehelfsmechanismus sowie darüber, dass sie nicht verpflichtet sind, davon Gebrauch zu machen oder bei der Einlegung eines Rechtsbehelfs eine bestimmte Reihenfolge einzuhalten.]

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

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.

([11]) Der Datenimporteur darf eine unabhängige Streitbeilegung über eine Schiedsstelle nur dann anbieten, wenn er in einem Land niedergelassen ist, das das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche ratifiziert hat.

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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

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) Jede Partei haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den die Partei der betroffenen Person verursacht, indem sie deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs gemäß der Verordnung (EU) 2016/679.

c) 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.

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

e) Der Datenimporteur kann sich nicht auf das Verhalten eines Auftragsverarbeiters oder Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung zu entziehen.

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche*(wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden)*

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. [In Bezug auf Modul drei: Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.]

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, [in Bezug auf Modul drei: gegebenenfalls in Absprache mit dem Verantwortlichen]. 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 [in Bezug Modul drei: vom Verantwortlichen oder] 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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche*(wenn der in der EU ansässige Auftragsverarbeiter die von dem im Drittland ansässigen Verantwortlichen erhaltenen personenbezogenen Daten mit personenbezogenen Daten kombiniert, die vom Auftragsverarbeiter in der EU erhoben wurden)*

([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.

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.

[In Bezug auf Modul drei: Der Datenexporteur leitet die Benachrichtigung an den Verantwortlichen weiter.]

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.). [In Bezug auf Modul drei: Der Datenexporteur leitet die Informationen an den Verantwortlichen weiter.]

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. [In Bezug auf Modul drei: Der Datenexporteur stellt die Beurteilung dem Verantwortlichen 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 [in Bezug auf Modul drei: und den Verantwortlichen] 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) [In Bezug auf die Module eins, zwei und drei: 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.] [In Bezug auf Modul vier: Von dem in der EU ansässigen Datenexporteur erhobene personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe c übermittelt wurden, müssen unverzüglich vollständig gelöscht werden, einschließlich aller Kopien.] 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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

[OPTION 1: Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von _____ (*Mitgliedstaat angeben*) ist.]

[OPTION 2 (in Bezug auf die Module zwei und drei): Diese Klauseln unterliegen dem Recht des EU-Mitgliedstaats, in dem der Datenexporteur niedergelassen ist. Wenn dieses Recht keine Rechte als Drittbegünstigte zulässt, unterliegen diese Klauseln dem Recht eines anderen EU-Mitgliedstaats, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von _____ (*Mitgliedstaat angeben*) ist.]

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Diese Klauseln unterliegen dem Recht eines Landes, das Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von _____ (*Land angeben*) ist.

Klausel 18

Gerichtsstand und Zuständigkeit

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

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 _____ (*Mitgliedstaat angeben*) 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.

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten von _____ (*Land angeben*) beigelegt.

ANLAGE

ERLÄUTERUNG:

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 Anlagen ausgefüllt und unterzeichnet werden müssen, sofern die geforderte Transparenz bei Verwendung einer einzigen Anlage erzielt werden kann. Erforderlichenfalls sollten getrennte Anlagen verwendet werden, um ausreichende Klarheit zu gewährleisten.

ANHANG I

A. **LISTE DER PARTEIEN**

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Datenexporteur(e): [*Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union*]

1. Name: .....

   Anschrift: .....

   Name, Funktion und Kontaktdaten der Kontaktperson: .....

   Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: .....

   Unterschrift und Datum: .....

   Rolle (Verantwortlicher/Auftragsverarbeiter): .....

2. .....

Datenimporteur(e): [*Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson*]

1. Name: .....

   Anschrift: .....

   Name, Funktion und Kontaktdaten der Kontaktperson: .....

   Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: .....

   Unterschrift und Datum: .....

   Rolle (Verantwortlicher/Auftragsverarbeiter): .....

2. .....

B. **BESCHREIBUNG DER DATENÜBERMITTLUNG**

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

.....

Kategorien der übermittelten personenbezogenen Daten

.....

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

.....

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

.....

Art der Verarbeitung

.....

Zweck(e) der Datenübermittlung und Weiterverarbeitung

.....

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

.....

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

.....

C. **ZUSTÄNDIGE AUFSICHTSBEHÖRDE**

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

Angabe der zuständigen Aufsichtsbehörde(n) gemäß Klausel 13

.....

ANHANG II

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

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret (nicht allgemein) beschrieben werden. Beachten Sie hierzu bitte auch die allgemeine Erläuterung auf der ersten Seite der Anlage; insbesondere ist klar anzugeben, welche Maßnahmen für jede Datenübermittlung bzw. jede Kategorie von Datenübermittlungen gelten.

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

[Beispiele für mögliche Maßnahmen:

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Maßnahmen zum Schutz der Daten während der Übermittlung

Maßnahmen zum Schutz der Daten während der Speicherung

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Maßnahmen zur Gewährleistung der Datenminimierung

Maßnahmen zur Gewährleistung der Datenqualität

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

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.

ANHANG III

LISTE DER UNTERAUFTRAGSVERARBEITER

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss für die Module zwei und drei im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 9 Buchstabe a, Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: .....

   Anschrift: .....

   Name, Funktion und Kontaktdaten der Kontaktperson: .....

   Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): .....

2. .....

COMMISSION IMPLEMENTING DECISION (EU) 2021/914

of 4 June 2021

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([1]), and in particular Article 28(7) and Article 46(2)(c) thereof,

Whereas:

(1) Technological developments are facilitating cross-border data flows necessary for the expansion of international cooperation and international trade. At the same time, it is necessary to ensure that the level of protection of natural persons guaranteed by Regulation (EU) 2016/679 is not undermined where personal data is transferred to third countries, including in cases of onward transfers ([2]). The data transfer provisions in Chapter V of Regulation (EU) 2016/679 are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country ([3]).

(2) Pursuant to Article 46(1) of Regulation (EU) 2016/679, in the absence of an adequacy decision by the Commission pursuant to Article 45(3), a controller or processor may transfer personal data to a third country only if it has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies for data subjects are available. Such safeguards may be provided for by standard data protection clauses adopted by the Commission pursuant to Article 46(2)(c).

(3) The role of standard contractual clauses is limited to ensuring appropriate data protection safeguards for international data transfers. Therefore, the controller or processor transferring the personal data to a third country (the 'data exporter') and the controller or processor receiving the personal data (the 'data importer') are free to include those standard contractual clauses in a wider contract and to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects. Controllers and processors are encouraged to provide additional safeguards by means of contractual commitments that supplement the standard contractual clauses ([4]). The use of the standard contractual clauses is without prejudice to any contractual obligations of the data exporter and/or importer to ensure respect for applicable privileges and immunities.

(4) Beyond using standard contractual clauses to provide appropriate safeguards for transfers pursuant to Article 46(1) of Regulation (EU) 2016/679, the data exporter has to fulfil its general responsibilities as controller or processor under Regulation (EU) 2016/679. Those responsibilities include an obligation of the controller to provide data subjects with information about the fact that it intends to transfer their personal data to a third country pursuant to Article 13(1)(f) and Article 14(1)(f) of Regulation (EU) 2016/679. In the case of transfers pursuant to Article 46 of Regulation (EU) 2016/679, such information must include a reference to the appropriate safeguards and the means by which to obtain a copy of them or information where they have been made available.

([1]) OJ L 119, 4.5.2016, p. 1.
([2]) Article 44 of Regulation (EU) 2016/679.
([3]) See also judgment of the Court of Justice of 16 July 2020 in Case C-311/18, *Data Protection Commissioner* v *Facebook Ireland Ltd and Maximillian Schrems ('Schrems II')*, ECLI:EU:C:2020:559, paragraph 93.
([4]) Recital 109 of Regulation (EU) 2016/679.

(5) Commission Decisions 2001/497/EC ([5]) and 2010/87/EU ([6]) contain standard contractual clauses to facilitate the transfer of personal data from a data controller established in the Union to a controller or processor established in a third country that does not offer an adequate level of protection. Those decisions were based on Directive 95/46/EC of the European Parliament and of the Council ([7]).

(6) Pursuant to Article 46(5) of Regulation (EU) 2016/679, Decision 2001/497/EC and Decision 2010/87/EU remain in force until amended, replaced or repealed, if necessary, by a Commission decision adopted pursuant to Article 46(2) of that Regulation. The standard contractual clauses in the decisions required updating in the light of new requirements in Regulation (EU) 2016/679. Moreover, since the decisions were adopted, the digital economy has seen significant developments, with the widespread use of new and more complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships. This calls for modernisation of the standard contractual clauses to reflect those realities better, by covering additional processing and transfer situations, and to allow a more flexible approach, for example with respect to the number of parties able to join the contract.

(7) A controller or processor may use the standard contractual clauses set out in the Annex to this Decision to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 for the transfer of personal data to a processor or controller established in a third country, without prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679. The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679. This also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 (pursuant to Article 3(2) thereof), because it relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union.

(8) Given the general alignment of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 of the European Parliament and of the Council ([8]), it should be possible to use the standard contractual clauses also in the context of a contract, as referred to in Article 29(4) of Regulation (EU) 2018/1725 for the transfer of personal data to a sub-processor in a third country by a processor that is not a Union institution or body, but which is subject to Regulation (EU) 2016/679 and which processes personal data on behalf of a Union institution or body in accordance with Article 29 of Regulation (EU) 2018/1725. Provided the contract reflects the same data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) Regulation (EU) 2018/1725, in particular by providing sufficient guarantees for technical and organisational measures to ensure that the processing meets the requirements of that Regulation, this will ensure compliance with Article 29(4) of Regulation (EU) 2018/1725. In particular, that will be the case where the controller and processor use the standard contractual clauses in Commission Implementing Decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([9]).

(9) Where the processing involves data transfers from controllers subject to Regulation (EU) 2016/679 to processors outside its territorial scope or from processors subject to Regulation (EU) 2016/679 to sub-processors outside its territorial scope, the standard contractual clauses set out in the Annex to this Decision should also allow to fulfil the requirements of Article 28(3) and (4) of Regulation (EU) 2016/679.

(10) The standard contractual clauses set out in the Annex to this Decision combine general clauses with a modular approach to cater for various transfer scenarios and the complexity of modern processing chains. In addition to the general clauses, controllers and processors should select the module applicable to their situation, so as to tailor their obligations under the standard contractual clauses to their role and responsibilities in relation to the data processing

([5]) Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181, 4.7.2001, p. 19).

([6]) Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5).

([7]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

([8]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39); see recital 5.

([9]) C(2021) 3701.

in question. It should be possible for more than two parties to adhere to the standard contractual clauses. Moreover, additional controllers and processors should be allowed to accede to the standard contractual clauses as data exporters or importers throughout the lifecycle of the contract of which they form a part.

(11) In order to provide appropriate safeguards, the standard contractual clauses should ensure that the personal data transferred on that basis is afforded a level of protection essentially equivalent to that guaranteed within the Union ([10]). With a view to ensuring transparency of processing, data subjects should be provided with a copy of the standard contractual clauses and be informed, in particular, of the categories of personal data processed, the right to obtain a copy of the standard contractual clauses, and any onward transfer. Onward transfers by the data importer to a third party in another third country should be allowed only if the third party accedes to the standard contractual clauses, if the continuity of protection is ensured otherwise, or in specific situations, such as on the basis of the explicit, informed consent of the data subject.

(12) With some exceptions, in particular as regards certain obligations that exclusively concern the relationship between the data exporter and data importer, data subjects should be able to invoke, and where necessary enforce, the standard contractual clauses as third-party beneficiaries. Therefore, while the parties should be allowed to choose the law of one of the Member States as governing the standard contractual clauses, that law must allow for third-party beneficiary rights. In order to facilitate individual redress, the standard contractual clauses should require the data importer to inform data subjects of a contact point and to deal promptly with any complaints or requests. In the event of a dispute between the data importer and a data subject who invokes his or her rights as a third-party beneficiary, the data subject should be able to lodge a complaint with the competent supervisory authority or refer the dispute to the competent courts in the EU.

(13) In order to ensure effective enforcement, the data importer should be required to submit to the jurisdiction of such authority and courts, and to commit to abide by any binding decision under the applicable Member State law. In particular, the data importer should agree to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. In addition, the data importer should have the option of offering data subjects the opportunity to seek redress before an independent dispute resolution body, at no cost. In line with Article 80(1) of Regulation (EU) 2016/679, data subjects should be allowed to be represented by associations or other bodies in disputes against the data importer if they so wish.

(14) The standard contractual clauses should provide for rules on liability between the parties and with respect to data subjects, and rules on indemnification between the parties. Where the data subject suffers material or non-material damage as a consequence of any breach of the third-party beneficiary rights under the standard contractual clauses, he or she should be entitled to compensation. This should be without prejudice to any liability under Regulation (EU) 2016/679.

(15) In the case of a transfer to a data importer acting as a processor or sub-processor, specific requirements should apply in accordance with Article 28(3) of Regulation (EU) 2016/679. The standard contractual clauses should require the data importer to make available all information necessary to demonstrate compliance with the obligations set out in the clauses and to allow for and contribute to audits of its processing activities by the data exporter. With respect to the engagement of any sub-processor by the data importer, in line with Article 28(2) and (4) of Regulation (EU) 2016/679, the standard contractual clauses should in particular set out the procedure for general or specific authorisation from the data exporter and the requirement for a written contract with the sub-processor ensuring the same level of protection as under the clauses.

(16) It is appropriate to provide different safeguards in the standard contractual clauses that cover the specific situation of a transfer of personal data by a processor in the Union to its controller in a third country and reflect the limited self-standing obligations for processors under Regulation (EU) 2016/679. In particular, the standard contractual clauses should require the processor to inform the controller if it is unable to follow its instructions, including if such instructions infringe Union data protection law, and require the controller to refrain from any actions that would prevent the processor from fulfilling its obligations under Regulation (EU) 2016/679. They should also require the parties to assist each other in responding to enquiries and requests from data subjects under the local law applicable

([10]) *Schrems II*, paragraphs 96 and 103. See also Regulation (EU) 2016/679, recitals 108 and 114.

to the data importer or, for data processing in the Union, under Regulation (EU) 2016/679. Additional requirements to address any effects of the laws of the third country of destination on the controller's compliance with the clauses, in particular how to deal with binding requests from public authorities in the third country for disclosure of the transferred personal data, should apply where the Union processor combines the personal data received from the controller in the third country with personal data collected by the processor in the Union. Conversely, no such requirements are justified where the outsourcing merely involves the processing and transfer back of personal data that has been received from the controller and in any event has been and will remain subject to the jurisdiction of the third country in question.

(17) The parties should be able to demonstrate compliance with the standard contractual clauses. In particular, the data importer should be required to keep appropriate documentation for the processing activities under its responsibility and to inform the data exporter promptly if it is unable to comply with the clauses, for whatever reason. In turn, the data exporter should suspend the transfer and, in particularly serious cases, have the right to terminate the contract, insofar as it concerns the processing of personal data under standard contractual clauses, where the data importer is in breach of the clauses or unable to comply with them. Specific rules should apply where local laws affect compliance with the clauses. Personal data that has been transferred prior to the termination of the contract, and any copies thereof, should at the choice of the data exporter be returned to the data exporter or destroyed in their entirety.

(18) The standard contractual clauses should provide for specific safeguards, in particular in the light of the case law of the Court of Justice ([11]), to address any effects of the laws of the third country of destination on the data importer's compliance with the clauses, in particular how to deal with binding requests from public authorities in that country for disclosure of the transferred personal data.

(19) The transfer and processing of personal data under standard contractual clauses should not take place if the laws and practices of the third country of destination prevent the data importer from complying with the clauses. In this context, laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679 should not be considered as being in conflict with the standard contractual clauses. The parties should warrant that, at the time of agreeing to the standard contractual clauses, they have no reason to believe that the laws and practices applicable to the data importer are not in line with these requirements.

(20) The parties should take account, in particular, of the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, the purpose of the processing), the laws and practices of the third country of destination that are relevant in light of the circumstances of the transfer and any safeguards put in place to supplement those under the standard contractual clauses (including relevant contractual, technical and organisational measures applying to the transmission of personal data and its processing in the country of destination). As regards the impact of such laws and practices on compliance with the standard contractual clauses, different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer.

(21) The data importer should notify the data exporter if, after agreeing to the standard contractual clauses, it has reason to believe that it is not able to comply with the standard contractual clauses. If the data exporter receives such notification or otherwise becomes aware that the data importer is no longer able to comply with the standard contractual clauses, it should identify appropriate measures to address the situation, if necessary in consultation with the competent supervisory authority. Such measures may include supplementary measures adopted by the data exporter and/or data importer, such as technical or organisational measures to ensure security and confidentiality. The data exporter should be required to suspend the transfer if it considers that no appropriate safeguards can be ensured, or if so instructed by the competent supervisory authority.

([11]) *Schrems II*.

(22) Where possible, the data importer should notify the data exporter and the data subject if it receives a legally binding request from a public (including judicial) authority under the law of the country of destination for disclosure of personal data transferred pursuant to the standard contractual clauses. Similarly, it should notify them if it becomes aware of any direct access by public authorities to such personal data, in accordance with the law of the third country of destination. If, despite its best efforts, the data importer is not in a position to notify the data exporter and/or the data subject of specific disclosure requests, it should provide the data exporter with as much relevant information as possible on the requests. In addition, the data importer should provide the data exporter with aggregate information at regular intervals. The data importer should also be required to document any request for disclosure received and the response provided, and make that information available to the data exporter or the competent supervisory authority, or both, upon request. If, following a review of the legality of such a request under the laws of the country of destination, the data importer concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the third country of destination, it should challenge it, including, where appropriate, by exhausting available possibilities of appeal. In any event, if the data importer is no longer able to comply with the standard contractual clauses, it should inform the data exporter accordingly, including where this is the consequence of a request for disclosure.

(23) As stakeholder needs, technology and processing operations may change, the Commission should evaluate the operation of the standard contractual clauses in the light of experience, as part of the periodic evaluation of Regulation (EU) 2016/679 referred to in Article 97 of that Regulation.

(24) Decision 2001/497/EC and Decision 2010/87/EU should be repealed three months after the entry into force of this Decision. During that period, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, still be able to use the standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU. For an additional period of 15 months, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, be able to continue to rely on standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU for the performance of contracts concluded between them before the date of repeal of those decisions, provided that the processing operations that are the subject matter of the contract remain unchanged and that reliance on the clauses ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679. In the event of relevant changes to the contract, the data exporter should be required to rely on a new ground for data transfers under the contract, in particular by replacing the existing standard contractual clauses with the standard contractual clauses set out in the Annex to this Decision. The same should apply to any sub-contracting to a (sub-)processor of processing operations covered by the contract.

(25) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered a joint opinion on 14 January 2021 ([12]), which has been taken into consideration in the preparation of this Decision.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679,

HAS ADOPTED THIS DECISION:

Article 1

1. The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer).

2. The standard contractual clauses also set out the rights and obligations of controllers and processors with respect to the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679, as regards the transfer of personal data from a controller to a processor, or from a processor to a sub-processor.

([12]) EDPB EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.

Article 2

Where the competent Member State authorities exercise corrective powers pursuant to Article 58 of Regulation (EU) 2016/679 in response to the data importer being or becoming subject to laws or practices in the third country of destination that prevent it from complying with the standard contractual clauses set out in the Annex, leading to the suspension or ban of data transfers to third countries, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.

Article 3

The Commission shall evaluate the practical application of the standard contractual clauses set out in the Annex on the basis of all available information, as part of the periodic evaluation required by Article 97 of Regulation (EU) 2016/679.

Article 4

1. This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. Decision 2001/497/EC is repealed with effect from 27 September 2021.

3. Decision 2010/87/EU is repealed with effect from 27 September 2021.

4. Contracts concluded before 27 September 2021 on the basis of Decision 2001/497/EC or Decision 2010/87/EU shall be deemed to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards.

Done at Brussels, 4 June 2021.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

([1]) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 **Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 **Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

([2]) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 **Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

([3]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

([4]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

MODULE THREE: Transfer processor to processor

8.1 **Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([5]).

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

([5]) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([6]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

([6]) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 **Instructions**

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 **Security of processing**

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data ([7]), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

([7]) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

([8]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([9]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

([9]) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([10]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

([10]) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([11]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

([11]) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

([12]) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*).

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. **LIST OF PARTIES**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: .....

Signature and date: .....

Role (controller/processor): .....

2. .....

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: .....

Signature and date: .....

Role (controller/processor): .....

2. .....

B. **DESCRIPTION OF TRANSFER**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.....

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.....

Nature of the processing

……

Purpose(s) of the data transfer and further processing

……

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

……

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

……

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

……

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, alsodescribe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ……

   Address: ……

   Contact person's name, position and contact details: ……

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ……

2. ……