Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

much. GmbH
Leopoldstraße 139
80804 München
Deutschland

und

–Auftragnehmer/Auftragsverarbeiter–

–Auftraggeber/Verantwortlicher–

Allgemeine Bestimmungen

1. Vertragsgegenstand

Dieser Vertrag zur Auftragsverarbeitung gemäß Art 28 DSGVO (nachfolgend **„Vertrag“**) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Gegenstand des Auftrags (Ziffer 4) in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte, personenbezogene Daten des Verantwortlichen verarbeiten.

2. Anwendung der EU Standardvertragsklauseln

Die Parteien legen diesem Vertrag die „Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR“ gemäß Durchführungsbeschluss der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28(7) DS-GVO und Artikel 29(7) der Verordnung (EU) 2018/1725 vom 4. Juni 2021 (nachfolgend **„EU Standardvertragsklauseln“**) zugrunde. Auf die Standardklauseln kann über folgenden Link zugegriffen werden. https://muchconsulting.de/agb-de/

Die Anlagen 1-4 sind Bestandteil dieser Vereinbarung.

Dabei vereinbaren die Parteien folgende in den EU Standardvertragsklauseln aufgeführten Optionen:

- Klausel 1: Option 1
- Klausel 7.7: Option 2 mit Einspruchsfrist von 14 Tagen.
- Klausel 8.c.4: Option 1
- Klausel 9.1.b: Option 1
- Klausel 9.1.c: Option 1
- Klausel 9.2: Option 1

3. Abweichungen von den EU Standardvertragsklauseln

Die Parteien vereinbaren folgende Abweichungen von den EU Standardvertragsklauseln. Diese Abweichungen kommen im Falle von Widersprüchen gegenüber den EU Standardklauseln vorrangig zur Anwendung.

3.1. Einsatz von Unterauftragsverarbeitern (Klausel 7.7)

Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht fristgerecht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Servicevertrag und diesen Vertrag zum nächstmöglichen Zeitpunkt zu kündigen.

3.2. Unterstützung des Verantwortlichen (Klausel 8)

Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen. Bei der Unterstützung finden die Tagessätze des Hauptvertrags (AGB nach §2.3 Dienstleistungen) Anwendung.

3.3. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten (Klausel 9.1)

Sofern der Auftragnehmer für die Verletzung des Schutzes von Auftraggeber-Daten nicht verantwortlich ist, kann der Auftragnehmer vom Auftraggeber Ersatz für die in Ausübung der Unterstützungsleistungen nachgewiesenen enstandenen Aufwände und Kosten verlangen.

4. Gegenstand des Auftrags

Im Rahmen der Leistungserbringung nach dem Hauptvertrag ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten Dritter umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen sowie die sich aus der besonderen Stellung des Auftraggebers als Berufsgeheimnisträger ergebenden Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

5. Dauer des Auftrags

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags, sofern in diesem Vertrag nicht Abweichendes geregelt ist. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

6. Umfang, Art und Zweck der Datenverarbeitung

Die Tätigkeit des Auftragnehmers dient dem Zweck, dem Auftraggeber verschiedene Leistungen im Zusammenhang mit dem Hosting der ERP-Plattform odoo sowie Dienstleistungen hieran zu erbringen und wird vom Auftragnehmer in dem im Hauptvertrag vereinbarten Umfang erbracht. Der Inhalt des mitgeltenden Anlagenverzeichnisses spezifiziert dabei Anforderungen an die Tätigkeit des Auftragnehmers. Dabei erbringt der Auftragnehmer die folgenden Leistungen:

- ☐ Hosting einer odoo-Plattform
- ☐ Dienstleistungen an den odoo-Systemen des Auftraggebers

Ort: München

Datum: _____

Ort: _____

Datum: _____

_____

_____

Auftragnehmer / Auftragsverarbeiter

Maximilian Rau, Geschäftsführer

Simon Stappen, Geschäftsführer

Auftraggeber/Verantwortlicher

Anlagenverzeichnis:

Anlage 1	Datenarten / Kreise von Betroffenen
Anlage 2	Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO
Anlage 3	Weitere Auftragsverarbeiter
Anlage 4	Verantwortliche Stelle, Datenschutzbeauftragter und weisungsberechtigte Personen

Datenarten / Kreise von Betroffenen (Anlage 1)

1. Vom Auftrag umfasste Datenarten

Folgende Datenarten sind üblicherweise Gegenstand dieses Auftrags.

- ☑ Name
- ☑ Adressdaten
- ☑ Telefonnummer
- ☑ E-Mails
- ☑ Kommunikationsdaten
- ☑ Geräteinformation
- ☐ Standort
- ☐ Kaufhistorie
- ☐ Zahlungsdaten
- ☐ Gehalt
- ☐ alle weiteren ggf. auf der odoo-Plattform des Auftraggebers gespeicherten Daten sind ggf vom Auftraggeber zu vervollständigen:

2. Kreise von Betroffenen

Folgende Kreise von Betroffenen sind Gegenstand des Auftrags:

- ☑ Beschäftigte des Auftraggebers
- ☑ Nutzer des Auftraggebers
- ☑ Kunden des Auftraggebers
- ☑ Interessenten des Auftraggebers
- ☑ Lieferanten und Dienstleister des Auftraggebers
- ☐ Auszubildende und Praktikanten des Auftraggebers
- ☐ Bewerber des Auftraggebers
- ☐ Betroffenenkreise sind ggf. vom Auftraggeber zu vervollständigen:

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO (Anlage 2)

Zum Zeitpunkt des Vertragsschlusses hat der Auftragnehmer folgende technisch organisatorischen Maßnahmen implementiert. Der Auftragnehmer ist aktuell ISO27001 und ISAE3402 SOC1 / SOC2 Zertifiziert.

Darüber hinaus werden alle Hosting Angebote in Rechenzentren der Hetzner Online GmbH betrieben. Ausführe Informationen zu Zutritts-, Zugangs-, Zugriffs-, Datenträger-, Trennungskontrolle, Integrität, Verfügbarkeit, Belastbarkeit finden Sie auch in den ToMs von Hetzner unter https://www.hetzner.com/AV/TOM.pdf.

I. Zweckbindung und Trennbarkeit
Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Logische Mandantentrennung (softwareseitig) in allen Softwaresystemen mit projektbasiertem Zugriffsmanagement
- Hosting Platform:
  - Trennung von Produktiv- und Testsystem auf unterschiedliche virtuelle Server
  - Logische Mandantentrennung durch virtuelle Server pro Kunde

II. Vertraulichkeit und Integrität
Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

1. Verschlüsselung
Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

- SSL bei Kommunikation über das Internet
- TLS 1.2+ / TLS 1.3 für alle Datenübertragungen (ältere Protokolle wie TLS 1.0/1.1, SSL, DES, 3DES, MD5, SHA-1 sind deaktiviert)
- AES-256 Verschlüsselung ruhender Daten (“at rest”)
- FileVault Full-Disk-Encryption auf allen Endgeräten
- SSH-Key-basierte Authentifizierung für Serverinfrastruktur
- Hosting-Plattform: SSL/TLS mit Let's Encrypt Zertifikaten

2. Pseudonymisierungs-Maßnahmen

- Der Auftraggeber ist für die Pseudonymisierung seiner Daten in den Anwendungen selbst verantwortlich.
- Für Testdatenbank ist einen Anonymisierung möglich mit dem kostenpflichtigen Anonymisierungsdienst

3. Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (**Zutrittskontrolle**):

Hosting: Rechenzentrum bei Hetzner Online GmbH

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenter-Park
- Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation Kunden für Colocation Racks
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters

Im Büro:

- Biometrisches oder mobile App mit biometrischen Freischaltung basiertes Schließsystem
- Aufzeichnung aller Zutritt mit digitaler Audit Trail für 90 Tage
- Videoüberwachung der Zugänge
- Keine Ausgabe von physischen Schlüsseln
- Sorgfältige Auswahl von Reinigungspersonal mit Kontrolle von polizeilichen Führungszeugnis beim Dienstleister

4. Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern **(Zugangskontrolle):**

- Zuordnung von Benutzerrechten, Zuordnung von Benutzerprofilen zu IT-Systemen
- Erstellen von Benutzerprofilen, Authentifikation mit Benutzername / Passwort, Passwortvergabe, Passwort-Richtlinien
- Nutzung von Passwort Managern, Single-Sign-On (“SSO”) und 2-Factor-Authentication (“2FA”)
- Zusätzliche Authentifizierung für alle Admins mit verpflichtenden FIDO-2 Schlüsseln
- RSA verschlüsselte SSH Keys bei Servern

- MDM verwaltet alle Endgeräte
- Endpoint Detection & Response (EDR) Lösung als Antivirus und Firewall auf allen Endgeräten
- Automatischen Sperrung von Endgeräten

5. Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**):

- Berechtigungskonzept Principle of Least Privilege
- Verwaltung der Rechte durch Systemadministrator
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte
- Dokumentierten On- & Offboarding und Rollenwechsel Prozess
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Sofortige Sperrung aller Zugänge bei Ausscheiden (Remote-Lock/Wipe)
- Passwortmanager, Single-Sign-On (“SSO”) und 2-Factor-Authentication (“2FA”)
- Lokales Speichern von Unternehmens-/Kundendaten nur auf verwalteten und verschlüsselten Firmengeräten
- Hosting: Trennung von Kunden in eigenen virtuelle Server

6. Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**).

- Umfassende Logs in allen Systemen mit Kundendaten
- Hosting
    - Änderungen werden auf Serverseite geloggt
    - Änderungen werden in der Applikation nachverfolgt und sind für andere Nutzer sichtbar
    - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**).

- ISO 27001:2022 zertifiziertes ISMS (Zertifikat gültig bis 08.02.2029)
- Speicherung aller Daten und Zugänge mit projektbasierten Zugriff
- Jährliche Managementbewertung und interne Audits
- Weisungen werden in Textform erteilt, sofern nicht anders im Hauptvertrag geregelt. Sollte eine Weisung aufgrund ihrer Dringlichkeit mündlich erteilt worden sein, wird der Auftraggeber sie unverzüglich schriftlich (oder: in Textform) nachsenden.
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnnis und Datenschutzschulungen
- Externer DSB (aktuell: Dr. Jochen Notholt) und jährliches DPO-Audit
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags gemäß Hauptvertrag

8. Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (**Transport- bzw. Weitergabekontrolle**):

- Ausschließliche Nutzung verschlüsselter Kanäle (HTTPS, verschlüsselte APIs)
- Credentials ausschließlich über 1Password Vaults oder über 2 End-2-End verschlüsselte Kanäle
- Keine Nutzung von USB-Sticks oder externen Datenträgern gestattet
- Transport und Weitergabe an Dritte nur aufgrund von einschlägigen Rechtsgrundlage und unter Anwendung angemessener Sicherheitsmaßnahmen wie
    - Einsatz von verschlüsselten “SSH-Tunneln”
    - Einsatz von verschlüsselte Übertragung (“SSL”)
    - Verschlüsselung physischer Datenträger

  weitergeben

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

- Hosting
    - Regelmäßige Updates der Software

- Täglich Backups mit Speicherung auf mindestens 2 redundanten Backup-Systemen. Es werden zu jedem Zeitpunkt mindestens fünf Backups aufbewahrt. Der Kunde trägt die Verantwortung, eigene Kopien der Backups anzufertigen.
- Regelmäßige Tests der Wiederherstellungsverfahren

IV. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen
Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen nach Ermessen oder anlassbezogen prüfen, evaluieren und bei Bedarf anpassen. Der in den TOM angegebene Sicherheitsstandard wird auch bei einer Anpassung der Maßnahmen zu keinem Zeitpunkt unterschritten.

Zusätzlich erfolgen fortlaufenden Management IT Security Reviews und ein jährliches externes ISO 27001 Audit.

Weitere Auftragsverarbeiter (Unterauftragnehmer) (Anlage 3)

Name und Anschrift der Unterauftragnehmer / weiteren Auftragsverarbeiter	**Gegenstand der Unterbeauftragung**	**Sitz des Auftragsverarbeiters**
Hetzner Online GmbH Industriestr 25 91710 Gunzenhausen	Hosting und Bereitstellung von Rechenzentrumsleistungen	Deutschland
much. Consulting - Unipessoal LDA, Av 5 de Outubro 146, 1050-061 Lisboa, Portugal (Tochter der much. GmbH)	Erbringen von Dienstleistungen gemäß Hauptvertrag	Portugal
Zukunft digitale und offene Verwaltung GmbH, Leopoldstraße 31,80802 München (Tochter der much. GmbH)	Erbringen von Dienstleistungen gemäß Hauptvertrag	Deutschland
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	Bereitstellung von Cloud Resourcen und Cloud-basierten Produktivitäts- und Kollaborationsdiensten (Google Workspace) mit Datenspeicherung innerhalb der EU, einschließlich E-Mail, Datenspeicherung, Kalender und Videokonferenzen, KI Interferenz im Rahmen der Dienstleistungen gemäß Hauptvertrag.	Ireland

Verantwortliche Stelle, Datenschutzbeauftragter und weisungsberechtigte Personen (Anlage 4)

Benennung der verantwortlichen Stelle zur Meldung nach Art. 12 bis 22 oder Art. 33 DSGVO
Im Falle eines Verstoßes gegen die genannten Artikel der DSGVO erfolgt die Meldung immer zuerst an die folgende Stelle:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18,
91504 Ansbach
Telefon: +49 (0) 981 180093-0
Telefax: +49(0) 981 180093-800
E-Mail: poststelle@lda.bayern.de

Nennung des ernannten Datenschutzbeauftragen des Auftragsverarbeiters
Der Auftragsverarbeiter hat folgende Person als Datenschutzbeauftragten bestellt:

Dr. Jochen Notholt Rechtsanwalt & DSB (TÜV)
Lindwurmstraße 10
80337 München
E-Mail: jn@comp-lex.de

Benennung weisungsberechtigter Personen
Die Benennung der weisungsberechtigten Personen erfolgt fortlaufend im Projekt zwischen den Parteien in Textform. Falls nicht anders geregelt, sind alle Geschäftsführer, Prokuristen und zusätzlich hier aufgelisteten Führungskräfte des Auftragsverarbeiters weisungsberechtigt:

Simon Stappen, Geschäftsführer, simon.stappen@muchconsulting.de
Maximilian Rau, Geschäftsführer, maximilian.rau@muchconsulting.de
Samuel Reinhardt, Prokurist, samuel.reinhardt@muchconsulting.de

In Notfällen auch an emergencies@muchconsulting.de wenden.

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/915 DER KOMMISSION

vom 4. Juni 2021

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

(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, DSGVO) ([1]), insbesondere auf Artikel 28 Absatz 7,

gestützt auf die 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 (EU-DSVO) ([2]), insbesondere auf Artikel 29 Absatz 7,

in Erwägung nachstehender Gründe:

(1) Die Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ spielen eine entscheidende Rolle bei der Anwendung der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725. Der Verantwortliche ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für die Zwecke der Verordnung (EU) 2018/1725 bezeichnet der Ausdruck „Verantwortlicher“ das Organ oder die Einrichtung der Union oder die Generaldirektion oder sonstige Organisationseinheit, das beziehungsweise die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten bestimmt. Sind die Zwecke und Mittel dieser Verarbeitung durch einen besonderen Rechtsakt der Union bestimmt, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien für seine Benennung nach dem Unionsrecht vorgesehen werden. Ein Auftragsverarbeiter ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(2) Für die Beziehung zwischen Verantwortlichen und Auftragsverarbeitern, die der Verordnung (EU) 2016/679 unterliegen, sollten dieselben Standardvertragsklauseln gelten – auch in dem Fall, wenn Verantwortliche und Auftragsverarbeiter unter die Verordnung (EU) 2018/1725 fallen. Grund ist, dass zur Gewährleistung einer einheitlichen Herangehensweise beim Schutz personenbezogener Daten in der gesamten Union und des freien Verkehrs personenbezogener Daten innerhalb der Union die Datenschutzbestimmungen in der Verordnung (EU) 2016/679, die für den öffentlichen Dienst in den Mitgliedstaaten gelten, und die Datenschutzbestimmungen in der Verordnung (EU) 2018/1725, die für die Organe, Einrichtungen und sonstigen Stellen der Union anwendbar sind, so weit wie möglich angeglichen wurden.

(3) Damit die Anforderungen der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 bei der Betrauung eines Auftragsverarbeiters mit Verarbeitungstätigkeiten eingehalten werden, sollte der Verantwortliche nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen der Verordnung (EU) 2016/679 und der Verordnung (EU) 2018/1725 genügen.

(4) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem die in Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 oder die in Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 aufgeführten Elemente festgelegt sind. Der Vertrag oder das Rechtsinstrument ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(5) Gemäß Artikel 28 Absatz 6 der Verordnung (EU) 2016/679 und Artikel 29 Absatz 6 der Verordnung (EU) 2018/1725 können der Verantwortliche und der Auftragsverarbeiter entweder einen individuellen Vertrag aushandeln, der die in Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 bzw. die in Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 aufgeführten obligatorischen Elemente enthält, oder Standardvertragsklauseln insgesamt oder teilweise verwenden, die von der Kommission gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 erlassen wurden.

([1]) ABl. L 119 vom 4.5.2016, S. 1.
([2]) ABl. L 295 vom 21.11.2018, S. 39.

(6) Dem Verantwortlichen und dem Auftragsverarbeiter sollte es freistehen, die in diesem Beschluss dargelegten 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 Anwendung der Standardvertragsklauseln gilt ungeachtet der vertraglichen Verpflichtungen des Verantwortlichen und/oder des Auftragsverarbeiters, die Einhaltung der geltenden Vorrechte und Befreiungen zu gewährleisten.

(7) Die Standardvertragsklauseln sollten sowohl materielle Rechte als auch Verfahrensrechte umfassen. Im Einklang mit Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 und Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 sollten die Standardvertragsklauseln den Verantwortlichen und den Auftragsverarbeiter auch verpflichten, den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der betreffenden personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegen.

(8) Gemäß Artikel 28 Absatz 3 der Verordnung (EU) 2016/679 und Artikel 29 Absatz 3 der Verordnung (EU) 2018/1725 muss der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren, wenn er der Auffassung ist, dass eine Anweisung des Verantwortlichen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(9) Wenn ein Auftragsverarbeiter einen anderen Auftragsverarbeiter zur Durchführung bestimmter Tätigkeiten in Anspruch nimmt, sollten die in Artikel 28 Absätze 2 und 4 der Verordnung (EU) 2016/679 oder in Artikel 29 Absätze 2 und 4 der Verordnung (EU) 2018/1725 verankerten speziellen Anforderungen Anwendung finden. Insbesondere ist eine vorherige gesonderte oder allgemeine schriftliche Genehmigung erforderlich. Unabhängig davon, ob es sich um eine gesonderte oder allgemeine Genehmigung handelt, sollte der erste Auftragsverarbeiter eine jeweils aktuelle Liste der anderen Auftragsverarbeiter führen.

(10) Zur Erfüllung der Anforderungen gemäß Artikel 46 Absatz 1 der Verordnung (EU) 2016/679 hat die Kommission Standardvertragsklauseln gemäß Artikel 46 Absatz 2 Buchstabe c der Verordnung (EU) 2016/679 erlassen. Diese Klauseln erfüllen auch die Anforderungen gemäß Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 für Datenübermittlungen von Verantwortlichen, die der Verordnung (EU) 2016/679 unterliegen, an Auftragsverarbeiter außerhalb des räumlichen Anwendungsbereichs dieser Verordnung oder von Auftragsverarbeitern, die der Verordnung (EU) 2016/679 unterliegen, an Unterauftragsverarbeiter außerhalb des räumlichen Anwendungsbereichs dieser Verordnung. Diese Standardvertragsklauseln können nicht als Standardvertragsklauseln im Sinne von Kapitel V der Verordnung (EU) 2016/679 verwendet werden.

(11) Dritte sollten die Möglichkeit haben, den Standardvertragsklauseln während der gesamten Laufzeit des Vertrags als Partei beizutreten.

(12) Die Anwendung der Standardvertragsklauseln sollte im Rahmen der nach Artikel 97 der Verordnung (EU) 2016/679 erforderlichen regelmäßigen Bewertung dieser Verordnung geprüft werden.

(13) 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 ([3]) abgegeben, die bei der Ausarbeitung des vorliegenden Beschlusses berücksichtigt wurde.

(14) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 93 der Verordnung (EU) 2016/679 und Artikel 96 Absatz 2 der Verordnung (EU) 2018/1725 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die im Anhang aufgeführten Standardvertragsklauseln erfüllen die Anforderungen an Verträge zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725.

Artikel 2

Die im Anhang aufgeführten Standardvertragsklauseln können in Verträgen zwischen einem Verantwortlichen und einem Auftragsverarbeiter, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, verwendet werden.

([3]) Gemeinsame Stellungnahme 1/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern für die in Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 genannten Angelegenheiten.

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 vorgesehenen regelmäßigen Bewertung.

Artikel 4

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

Brüssel, den 4. Juni 2021

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

Standardverstragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von [zutreffende Option auswählen: OPTION 1: Artikel 28 Absätze 3 und 4 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)] oder [OPTION 2: Artikel 29 Absätze 3 und 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] sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. **Weisungen**

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. **Zweckbindung**

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. **Dauer der Verarbeitung personenbezogener Daten**

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. **Sicherheit der Verarbeitung**

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten 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 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 den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

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

7.5. **Sensible Daten**

Falls die Verarbeitung personenbezogene Daten betrifft, 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 Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. **Dokumentation und Einhaltung der Klauseln**

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

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. **Einsatz von Unterauftragsverarbeitern**

a) OPTION 1: VORHERIGE GESONDERTE GENEHMIGUNG: Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens [ZEITRAUM ANGEBEN] vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

OPTION 2: ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter 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 betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen 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 Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. **Internationale Datenübermittlungen**

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß [OPTION 1: Artikel 32 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 33 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725].

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. **Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß [OPTION 1: Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 34 Absatz 3 der Verordnung (EU) 2018/1725] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese 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;

c) bei der Einhaltung der Pflicht gemäß [OPTION 1: Artikel 34 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 35 der Verordnung (EU) 2018/1725], die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. **Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten**

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese 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.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß [OPTION 1: Artikel 33 und 34 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 34 und 35 der Verordnung (EU) 2018/1725] zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

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

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANHANG I

Liste der Parteien

Verantwortliche(r): [*Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen*]

1. Name: .....

Anschrift: .....

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

Unterschrift und Beitrittsdatum: .....

2.

.....

Auftragsverarbeiter: [*Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters*]

1. Name: .....

Anschrift: .....

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

Unterschrift und Beitrittsdatum: .....

2.

.....

ANHANG II

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

.....

Kategorien personenbezogener Daten, die verarbeitet werden

.....

Verarbeitete 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

.....

Art der Verarbeitung

.....

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

.....

Dauer der Verarbeitung

.....

.....

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

ANHANG III

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung ist nicht ausreichend.

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (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 ergreifen muss.

Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss

ANHANG IV

Liste der Unterauftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 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. .....