Auftragsdatenverarbeitungsvertrag

Dieser Auftragsdatenverarbeitungsvertrag („AV-Vertrag“)
ist geschlossen zwischen:

Mustermann GmbH
Max Mustermann
mit Hauptgeschäftssitz in
Musterstraße 12
12345 Musterstadt, Deutschland

(„Verantwortlicher“)

und

RedGecko GmbH
mit Hauptgeschäftssitz am
Paul-Lincke-Ufer 20
10999 Berlin, Deutschland

(„Auftragsverarbeiter“ oder „Diensteanbieter“)

jeweils einzeln „Partei“, zusammen die „Parteien“.

PRÄAMBEL

Leistungsumfang des Auftragsverarbeiters ist die Bereitstellung eines Service-Tools (das Tool) zur Übermittlung von Artikeln aus angebundenen Onlineshops in Online-Verkaufsplattformen (Marktplatz) wie z. B. eBay oder Amazon. Des Weiteren überträgt das Tool optional Bestellungen aus den Verkaufsplattformen in den Onlineshop und synchronisiert Daten wie Preise oder Lagerbestände. Datenbasis ist im Kern der Onlineshop und der Marktplatz.
Der Verantwortliche betreibt einen Onlineshop oder verwendet eine Software, in den oder in die Teile des Tools durch den Verantwortlichen selbst, oder im Auftrag des Verantwortlichen installiert werden, sofern das Tool nicht bereits in dem Onlineshop oder der Software gebundelt ausgeliefert wurde.

Gemäß dem zwischen den Parteien geschlossenen Vertrages vom 16.07.2012 (der „Servicevertrag“), hat sich der Diensteanbieter verpflichtet, die in Anhang 1 zu diesem AV-Vertrag näher beschriebenen Dienste gegenüber dem Verantwortlichen zu erbringen (die „Dienste“).

Im Rahmen der Diensteerbringung kann es vorkommen, dass dem Diensteanbieter Personenbezogene Daten oder persönliche Informationen des Verantwortlichen im Sinne des anwendbaren Datenschutzrechts zur Verfügung gestellt werden oder er Zugriff auf diese erhält;

Der Diensteanbieter ist im Auftrag des Verantwortlichen als Auftragsverarbeiter tätig. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Servicevertrag (und der dazugehörigen Leistungsbeschreibung). Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Die Bestimmungen aus diesem AV-Vertrag finden Anwendung auf alle Tätigkeiten, die mit dem Servicevertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

Dieser AV-Vertrag beinhaltet die Bestimmungen, die auf die Erhebung, Verarbeitung und Nutzung der Personenbezogenen Daten durch den Diensteanbieter als vom Verantwortlichen beauftragter Auftragsverarbeiter Anwendung finden, um sicherzustellen, dass die Parteien in Übereinstimmung mit anwendbarem Datenschutzrecht handeln.

Um eine rechtskonforme Ausgestaltung ihrer Beziehung zu ermöglichen, haben die Parteien den AV-Vertrag wie folgt geschlossen, wobei deren Erfüllung nicht gesondert vergütet wird:

1. Definitionen

Für die Zwecke dieses AV-Vertrags:

„Anwendbares Datenschutzrecht“

meint die auf den Verantwortlichen und den Auftragsverarbeiter anwendbaren Rechtsvorschriften zum Schutz der Grundrechte und Freiheiten der Einzelnen und insbesondere deren Recht auf Privatsphäre in Bezug auf die Verarbeitung ihrer Personenbezogenen Daten; der Begriff anwendbares Datenschutzrecht umfasst die DSGVO ab dem 25. Mai 2018;

„Verantwortlicher“
meint diejenige Stelle, die als Rechtsperson alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Personenbezogenen Daten entscheidet;

„Datenschutzgrundverordnung“ oder „DSGVO“
meint die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die ab dem 25. Mai 2018 gilt;

„Mitgliedstaat“
meint einen Staat, der Mitglied der EU ist;

„Personenbezogene Daten“
meint alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („Betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

„Verletzung des Schutzes Personenbezogener Daten“
meint eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust oder zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise Verarbeitet wurden;

„Verarbeiten/Verarbeitung“
meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„Auftragsverarbeiter“
meint den Diensteanbieter, der Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

„Besondere Kategorien Personenbezogener Daten“
meint Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;

„Unterauftragsverarbeiter“
meint einen Auftragsverarbeiter, der im Auftrag des Diensteanbieters tätig ist und sich bereit erklärt, vom Diensteanbieter Personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese für den Verantwortlichen nach dessen Anweisungen, den Bestimmungen dieses AV-Vertrags (einschließlich der Standardvertragsklauseln, sofern diese Anwendung finden) und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

„Aufsichtsbehörde“
meint eine von einem Mitgliedstaat gemäß Artikel 51 DSGVO eingerichtete unabhängige staatliche Stelle; und

„Technische und Organisatorische Maßnahmen“ oder „TOMs“
meint solche Maßnahmen zum Schutze Personenbezogener Daten gegen unbeabsichtigte Zerstörung oder unbeabsichtigten Verlust, Veränderung, unautorisierte Offenlegung oder unautorisierten Zugriff, insbesondere wenn die Verarbeitung die Übermittlung von Daten über ein Netzwerk beinhaltet, sowie gegen alle sonstigen unrechtmäßigen Arten der Verarbeitung.

2. Einzelheiten der Verarbeitung

Die Einzelheiten der vom Auftragsverarbeiter für den Verantwortlichen erbrachten Verarbeitungshandlungen (z.B. der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Arten der Personenbezogenen Daten und Kategorien von Betroffenen Personen) ergeben sich aus Anhang 1 zu diesem Vertrag.

3. Rechte und Pflichten des Verantwortlichen

a. Der Verantwortliche bleibt die für die Verarbeitung der Personenbezogenen Daten verantwortliche Stelle.

b. Der Verantwortliche ist berechtigt und verpflichtet, dem Auftragsverarbeiter im Zusammenhang mit der Verarbeitung der Personenbezogenen Daten allgemeine oder auf den Einzelfall bezogene Weisungen zu erteilen. Weisungen können sich auch auf die Berichtigung, die Löschung oder das Sperren von Personenbezogenen Daten beziehen. Auf Nachfrage hat der Verantwortliche seine Weisungen, Instruktionen und Anmerkungen zu präzisieren. Weisungen hat der Verantwortliche schriftlich zu dokumentieren.

4. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter ist verpflichtet,

a. ausschließlich dokumentierte Weisungen des Verantwortlichen im Hinblick auf die Verarbeitung Personenbezogener Daten im Auftrag zu befolgen. Diese Verpflichtung gilt auch im Hinblick auf die Übermittlung Personenbezogener Daten in einen Drittstaat. Sofern der Auftragsverarbeiter nach EU-Recht oder dem Recht eines Mitgliedstaats, das auf den Auftragsverarbeiter anwendbar ist, verpflichtet ist, Personenbezogene Daten in einen Drittstaat zu übermitteln, teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weisungen werden im Servicevertrag, diesem AV-Vertrag und/oder sonst in dokumentierter Form erteilt.

b. Personenbezogene Daten für keinen anderen Zweck zu verarbeiten, als zur Erbringung der Dienste gegenüber dem Verantwortlichen.

c. den Verantwortlichen sofort zu informieren, sofern der Auftragsverarbeiter der Meinung ist, eine Weisung des Verantwortlichen verstoße gegen anwendbares Datenschutzrecht und diesen aufzufordern, die entsprechende Weisung zurückzunehmen, abzuändern oder zu bestätigen. Der Auftragsverarbeiter ist berechtigt, die Umsetzung der entsprechenden Weisung auszusetzen, solange die Entscheidung über die Rücknahme, Änderung oder Bestätigung der Weisung aussteht.

d. sicherzustellen, dass Personen, die vom Auftragsverarbeiter befugt sind, Personenbezogene Daten für den Verantwortlichen zu verarbeiten, im Hinblick auf das anwendbare Datenschutzrecht angemessen informiert, geschult und angewiesen sind und sich schriftlich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragsverarbeiter wird sicherstellen, dass solche befugten Personen das anwendbare Datenschutzrecht auch nach deren jeweiliger Beschäftigungszeit beachten.

e. bevor Personenbezogene Daten verarbeitet werden, die in Anhang 2 näher beschriebenen, den Anforderungen des anwendbaren Datenschutzrechts entsprechenden Technischen und Organisatorischen Maßnahmen umzusetzen und sicherzustellen, dass diese Technischen und Organisatorischen Maßnahmen dem Verantwortlichen ausreichende Garantien bieten.

f. den Verantwortlichen im Rahmen des Möglichen durch angemessene Technische und Organisatorische Maßnahmen bei der Erfüllung der Pflicht des Verantwortlichen zur Beantwortung von Anfragen in Ausübung der Betroffenenrechte betreffend Information, Auskunft, Berichtigung und Löschung, Einschränkung der Verarbeitung, Benachrichtigung, Datenübertragbarkeit, Widerspruch und automatisierte Entscheidungen, zu unterstützen.

g. Maßnahmen zu ergreifen, die der Verantwortliche zur Erfüllung der Rechte der Betroffenen Personen gemäß anwendbarem Datenschutzrecht anfordert oder anweist. Insbesondere muss der Auftragsverarbeiter Informationen über die auf Antrag ergriffenen Maßnahmen ohne schuldhaftes Zögern beziehungsweise zeitnah zur Verfügung stellen.

h. dem Verantwortlichen alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der Bestimmungen dieses AV-Vertrags und Art. 28 DSGVO nachzuweisen.

i. Audits zu ermöglichen und daran mitzuwirken, einschließlich Überprüfungen, die der Verantwortliche oder ein anderer vom Verantwortlichen beauftragter Prüfer vornimmt.

j. den Verantwortlichen unverzüglich zu informieren:

(i) über jegliche bindende Anfrage einer Strafverfolgungsbehörde auf Offenlegung Personenbezogener Daten, sofern dies nicht anderweitig verboten ist, bspw. aufgrund eines strafrechtlichen Verbots zum Schutze der Vertraulichkeit des Ermittlungsverfahrens.

(ii) über unmittelbar an ihn adressierte Beschwerden und Anfragen betroffener Personen (bspw. im Hinblick auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch gegen die Datenverarbeitung, automatisierte Entscheidungsfindung), ohne solche Anfragen zu beantworten, sofern er nicht hierzu ermächtigt wurde.

(iii) nachdem der Auftragsverarbeiter von einer Verletzung des Schutzes Personenbezogener Daten beim Auftragsverarbeiter oder bei seinem Unterauftragsverarbeiter Kenntnis erlangt hat. Im Falle einer solchen Verletzung des Schutzes Personenbezogener Daten wird der Auftragsverarbeiter den Verantwortlichen bei der Aufklärung der Verletzung des Schutzes Personenbezogener Daten und der Erfüllung der Pflicht des Verantwortlichen zur Benachrichtigung der Betroffenen Personen und der Aufsichtsbehörde, soweit eine solche jeweils besteht, unterstützen und die Verletzung des Schutzes Personenbezogener Daten dokumentieren.

k. den Verantwortlichen bei jeglicher Datenschutzfolgenabschätzung und vorherigen Konsultation, soweit anwendbar, zu unterstützen, die sich auf die von dem Auftragsverarbeiter für den Verantwortlichen erbrachten Dienste und die im Auftrag des Verantwortlichen verarbeiteten Personenbezogenen Daten beziehen.

l. Zuständige Aufsichtsbehörde für den Verantwortlichen teilt der Verantwortliche dem Auftragsverarbeiter schriftlich mit. Zuständige Aufsichtsbehörde für den Auftragsverarbeiter ist der Berliner Beauftragte für den Datenschutz und Informationsfreiheit.

m. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

n. Beim Auftragsverarbeiter ist als betrieblicher Datenschutzbeauftragter bestellt: Christian Scholz, interner Datenschutzbeauftragter der RedGecko GmbH, Telefon: +49 (0) 30 / 120 76 74 12, E-Mail: datenschutz@redgecko.de.

5. Unterauftragsverarbeitung

a. Jeglicher Unterauftrag mit einem Dritten, durch den die Erbringung der Dienste oder Teile davon auf einen Dritten übertragen wird, ist nur mit vorheriger für den Einzelfall oder allgemein erteilter schriftlicher Zustimmung des Verantwortlichen zulässig und muss in Schriftform, einschließlich der elektronischen Form, geschlossen werden.

b. Im Falle einer allgemein erteilten schriftlichen Zustimmung ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen über jede beabsichtigte Änderung im Hinblick auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern zu informieren, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

c. Der Auftragsverarbeiter ist verpflichtet, vertraglich sicherzustellen, dass der Unterauftragsverarbeiter im Hinblick auf die unterbeauftragten Dienste denselben Pflichten gegenüber dem Verantwortlichen unterliegt, insbesondere dass der Unterauftragsverarbeiter hinreichende Garantien bietet, dass geeignete Technische und Organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung den Anforderungen des anwendbaren Datenschutzrechts genügt.

d. Sofern der Unterauftragsverarbeiter seinen datenschutzrechtlichen Pflichten nicht nachkommt, bleibt der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Erfüllung der Pflichten des Unterauftragsverarbeiters uneingeschränkt verantwortlich.

e. Der Verantwortlichen ist berechtigt, Audits unmittelbar gegenüber dem Unterauftragsverarbeiter durchzuführen und diesem unmittelbare Weisungen zu erteilen. Der Verantwortliche ist berechtigt, eine Kopie des Unterauftrags zu verlangen.

f. Der Auftragsverarbeiter hat den Unterauftragsverarbeiter sorgfältig auszuwählen.

g. Sofern ein Unterauftragsverarbeiter außerhalb der EU/des EWR in einem Staat niedergelassen ist, der nicht als ein Staat anerkannt ist, in dem ein angemessenes Datenschutzniveau gewährt wird, wird der Auftragsverarbeiter auf schriftliches Verlangen des Verantwortlichen, im Auftrag des Verantwortlichen (im Namen des Verantwortlichen) die Standardvertragsklauseln (Controller to Processor) mit dem entsprechenden Unterauftragsverarbeiter abschließen. In diesem Fall erteilt der Verantwortliche dem Auftragsverarbeiter die Weisung und ermächtigt diesen, den Unterauftragsverarbeiter im Namen des Verantwortlichen anzuweisen und alle dem Verantwortlichen nach den Standardvertragsklauseln zustehenden Rechte gegenüber dem Unterauftragsverarbeiter auszuüben.

Genehmigte Unterauftragsverarbeiter sind in Anhang 3 aufgeführt. Die technisch-organisatorischen Maßnahmen, zu denen sich die Unterauftragsverarbeiter gegenüber dem Auftragsverarbeiter verpflichtet haben und die der Auftragsverarbeiter dadurch umsetzt sind in Anhang 3 genannt und als Anlagen dem AV-Vertrag beigefügt.

6. Laufzeit und Kündigung

a. Die Laufzeit dieses AV-Vertrags entspricht der Laufzeit des entsprechenden Servicevertrags. Sofern hierin nicht anders geregelt, gelten die im Servicevertrag niedergelegten Kündigungsrechte und Voraussetzungen entsprechend.

b. Der Diensteanbieter hat, nach Wahl des Verantwortlichen, alle Personenbezogenen Daten des Verantwortlichen nach dem Ende der Diensterbringung zu löschen oder an den Verantwortlichen zurück zu geben und alle bestehenden Kopien zu löschen, soweit nicht EU-Recht oder das Recht eines Mitgliedstaats den Diensteanbieter verpflichtet, solche Personenbezogenen Daten aufzubewahren.

7. Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter alleine der Verantwortliche gegenüber dem Betroffenen verantwortlich.

8. Sonstiges

a. Die Präambel und die Annexe - auch die Anlagen und TOMs der Unterauftragsdatenverarbeiter - sind integraler Bestandteil dieses AV-Vertrags.

b. Sollte sich eine Bestimmung dieses AV-Vertrags als unwirksam oder undurchsetzbar erweisen, berührt dies die Wirksamkeit der übrigen Bestimmungen dieses AV-Vertrags nicht. In einem solchen Fall wird die unwirksame oder undurchsetzbare Bestimmung automatisch durch eine wirksame und durchsetzbare Bestimmung ersetzt, die so weit wie möglich dem Zweck der ursprünglichen Bestimmung entspricht. Dies gilt entsprechend im Falle einer unbeabsichtigten Lücke dieses AV-Vertrags.

c. Die Regelungen dieses AV-Vertrags gehen im Konfliktfall den Regelungen des Servicevertrages vor.

d. Dieser AV-Vertrag unterliegt demselben Recht wie der Servicevertrag.

e. Der Streitlösungsmechanismus des Servicevertrages findet auch Anwendung auf diesen AV-Vertrag.

f. Die deutsche Sprachfassung dieses AV-Vertrags geht der englischen Sprachfassung vor.

Für den Verantwortlichen

Max Mustermann

Geschäftsführer

Digital signiert, Mustermann GmbH
Musterstadt, 29.05.2018

Für den Auftragsverarbeiter:

Peter Mähner & Semira Stark

Managing Partner

Digital signiert, RedGecko GmbH
Berlin, 01.06.2018

Anhang 1

Einzelheiten der Datenverarbeitung

1. Gegenstand der Verarbeitung

Leistungsumfang des Auftragsverarbeiters ist die Bereitstellung eines Service-Tools (das Tool) zur Übermittlung von Artikeln aus angebundenen Onlineshops in Online-Verkaufsplattformen wie z. B. eBay oder Amazon. Des Weiteren überträgt das Tool optional Bestellungen aus den Verkaufsplattformen in den Onlineshop und synchronisiert Daten wie Preise oder Lagerbestände. Datenbasis ist im Kern der Onlineshop und der Marktplatz.

2. Art und Zweck der Verarbeitung

Der Verantwortliche kann in der Konfiguration des Tools einen Bestellimport aktivieren, der dann Käuferbestellungen aus dem jeweils konfigurierten Marktplatz in seine Software oder Webshop importiert. Das Tool importiert und verarbeitet dabei die Bestellungen auf Servern des Auftragsverarbeiters auf eine solche Art und Weise, dass sie von der Software oder dem Webshop des Verantwortlichen weiter importiert und dort angezeigt werden können.

3. Kategorien der betroffenen Personen

Die übermittelten Personenbezogenen Daten betreffen die folgenden betroffenen Personen:

Käufer, die auf den über das Tool angebundenen Marktplätzen Bestellungen tätigen:
Sofern der Verantwortliche die im Tool vorhandene Bestellimport-Funktion vom Marktplatz zu seiner Software oder seinem Onlineshop aktiviert hat, werden Personenbezogene Daten vom Marktplatz übermittelt.

4. Arten Personenbezogener Daten

Die vom Auftragsverarbeiter für den Verantwortlichen verarbeiteten Personenbezogenen Daten betreffen die folgenden Kategorien Personenbezogener Daten:

- Käuferanschrift
- Rechnungsanschrift
- Lieferadresse
- Zahlart (jedoch keine Informationen über seine Zahlmethode wie Kontoverbindung oder Kreditkartendaten).

5. Besondere Kategorien von Daten

Die vom Auftragsverarbeiter für den Verantwortlichen verarbeiteten Personenbezogenen Daten betreffen die folgenden besonderen Kategorien von Daten: Nicht anwendbar

Anhang 2

Technische und Organisatorische Maßnahmen

Allgemeine technische und organisatorische Sicherheitsmaßnahmen des Auftragsverarbeiters

I. Vertraulichkeit (Art. 32 Abs. 1 lit b DSGVO)

1. Kontrolle des Zutritts zu Verarbeitungsbereichen

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um zu verhindern, dass unberechtigte Personen Zutritt zu Datenverarbeitungsanlagen, mit deren Hilfe Personenbezogene Daten verarbeitet werden, erhalten. Dies wird auf folgende Weise erreicht:

- Der Zutritt zu den Gebäuden wird von Sicherheitskräften zwischen Gebäudeeingang und dem Zugang zum Büro kontrolliert. Die Kontrolle findet während der Bürozeiten, spätestens bis 22:00 Uhr Abends statt. Nachdem die Sicherheitskräfte ihre Kontrollen beendet haben, werden die Haupteingänge verschlossen. Die Sicherheitskräfte und Maßnahmen werden vom Eigentümer gestellt.
- Der Sicherheitsdienst prüft nach Bürozeiten durch Rundgang, ob alle Türen und Fenster verschlossen sind und ob sich Personen im Gebäude und den Büroflächen befinden, die keinen berechtigten Zutritt haben.
- Videoüberwachung wird ausserhalb der Bürozeiten innerhalb der Büroflächen verwendet. Bewegungsmelder erkennen Zutritt während dieser Zeiten und senden Warn-Nachrichten and zuständige Mitarbeiter des Auftragsverarbeiters.
- Besuchern des Auftragsverarbeiters wird der Zutritt nur in Begleitung gewährt;
- Regelungen und Verzeichnisse für Schlüsseltransponder;
- Beschränkungen für Schlüsseltransponder;
- Protokollierung der Schlüsseltransponder

2. Kontrolle des Zugangs zu Datenverarbeitungssystemen

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um seine Datenverarbeitungssysteme vor Nutzung durch unberechtigte Personen zu schützen. Dies wird auf folgende Weise erreicht:

- Benutzer bekommen eigene Anmeldedaten; Passwörter müssen Regeln bzgl. Länge, Komplexität, Erneuerung und Verlauf befolgen;
- Identifizierung des Terminals und/oder des Terminalnutzers der Systeme des Auftragsverarbeiters;
- Automatische Zeitablauf-Funktion des Nutzerterminals bei Untätigkeit, Identifizierung und Passwort erforderlich zur erneuten Öffnung;
- Einsatz von individuellen Terminals und/oder Terminalnutzern, Identifikationskriterien exklusiv für spezielle Funktionen - z. B. SSH-Keys;
- Mitarbeiterrichtlinien im Hinblick auf die Zugangsrechte jedes Mitarbeiters zu Personenbezogenen Daten (sofern der Fall), Schulung der Mitarbeiter über ihre Pflichten und die Konsequenzen bei Verletzung der Pflichten, um sicherzustellen, dass die Mitarbeiter nur auf Personenbezogene Daten und Mittel zugreifen, die erforderlich sind, um beruflichen Pflichten nachzukommen;
- Schulung der Mitarbeiter über ihre datenschutzrechtlichen Pflichten und Verantwortlichkeiten;
- Protokollierung des Zugangs zu Daten im Rahmen der Auftragsdatenverarbeitung;
- Nutzung von Verschlüsselungstechnologien, die dem Stand der Technik entsprechen.

3. Kontrolle des Zugriffs auf besonderer Bereiche von Datenverarbeitungssystemen

Der Auftragsverarbeiter verpflichtet sich sicherzustellen, dass die zur Nutzung seiner Datenverarbeitungssysteme berechtigten Personen ausschließlich insoweit auf Daten zuzugreifen können, wie dies von Umfang und Ausmaß ihrer Nutzungserlaubnis (Berechtigung) gedeckt ist und, dass Personenbezogene Daten ohne Berechtigung nicht gelesen, vervielfältigt, verändert oder gelöscht werden können. Dies wird auf folgende Weise erreicht:

- Die Mitarbeiter des Auftragsverarbeiters bekommen minimale Zugangsrechte abhängig von ihren beruflichen Anforderungen;
- Berechtigungsrollen im Hinblick auf die Zugangsrechte jedes Mitarbeiters zu den Personenbezogenen Daten;
- Zuordnung von individuellen Terminals und/oder Terminalnutzern, und Identifikationskriterien exklusiv für spezielle Funktionen;
- Überwachungsmöglichkeit im Hinblick auf Personen, die Personenbezogene Daten löschen, ergänzen oder verändern können und zumindest jährliche Überwachung und Aktualisierung der Berechtigungsprofile;

- Freigabe von Daten nur an autorisierte Personen;
- Richtlinien, welche die Aufbewahrung von Sicherungskopien regeln; und
- Nutzung von Verschlüsselungstechniken, die dem Stand der Technik entsprechen.

4. Trennung der Verarbeitung für verschiedene Zwecke

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um sicherzustellen, dass für verschiedene Zwecke erhobene Daten getrennt voneinander verarbeitet werden können. Dies wird auf folgende Weise erreicht:

- Der Zugriff auf Daten ist durch die Sicherheitseinstellungen der Anwendung für die entsprechenden Nutzer getrennt;
- Auf der Datenbank-Ebene werden Daten getrennt nach Modulen oder unterstützter Funktion in unterschiedlichen Bereichen gespeichert. Insbesondere Entwicklungs- und Live-Umgebungen;
- und Schnittstellen, Batch-Prozesse und Berichte sind nur für bestimmte Zwecke und Funktionen konzipiert, sodass Daten, die für bestimmte Zwecke erhoben wurden, getrennt voneinander verarbeitet werden - insbesondere Entwicklungs- und Live-Umgebungen.

5. Pseudonymierung

Um die festgelegten Zwecke der Auftragsdatenverarbeitung zu erreichen, ist es nicht möglich die Personenbezogenen Daten zu pseudonymisieren.

6. Verschlüsselung

Die Personenbezogenen Daten sind im IT-System (siehe auch „Unterauftragsverarbeiter“) des Auftragsverarbeiters gespeichert und werden an den Auftragsverarbeiter über diese IT-Infrastruktur übertragen. Daher ist der Auftragsverarbeiter dafür verantwortlich, die Verschlüsselung der Personenbezogenen Daten bei Speicherung und während der Übertragung sicherzustellen.

II. Integrität (Art. 32 Abs.1, lit b DSGVO)

1. Eingabekontrolle

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um sicherzustellen, dass es möglich ist, zu prüfen und festzustellen, ob und wer Personenbezogene Daten in Datenverarbeitungssysteme eingegeben oder hieraus entfernt hat. Dies wird auf folgende Weise erreicht:

- Authentifizierung der berechtigten Mitarbeiter; individuelle Authentifizierungsdaten, wie SSH-Keys oder Benutzernamen, die wenn sie einmal zugewiesen wurden, nicht einer anderen Personen zugewiesen können;
- Einsatz von Nutzerkennungen (Passwörtern), mit zumindest acht Zeichen oder eine maximal zulässige Anzahl und Änderung bei der ersten Nutzung und danach zumindest alle 90 Tage im Falle von Verarbeitung von sensiblen Daten;
- Beachten einer Richtlinie, nach der alle Mitarbeiter des Auftragsverarbeiters, die Zugang zu den für den Auftragsgeber verarbeiteten Personenbezogenen Daten haben, ihre Passwörter zumindest einmal im Zeitraum von 180 Tagen zurücksetzen müssen;
- Dafür sorgen, dass der Zugang zu den Datenverarbeitungsgebäuden (die Räume, in denen sich die Computer Hardware und zugehörige Ausrüstung befinden) verschlossen werden kann;
- Automatisches Ausloggen von Nutzer-IDs (Erfordernis einer erneuten Passworteingabe, um den entsprechenden Arbeitsplatz zu nutzen), die für einen erheblichen Zeitraum nicht benutzt wurden;
- Deaktivierung von Nutzer Authentifizierungsdaten (wie zum Beispiel der Nutzer-ID), wenn die Person von der Verarbeitung von Personenbezogenen Daten ausgeschlossen wird oder wenn sie einen erheblichen Zeitraum (zumindest sechs Monate) nicht genutzt werden, ausschließlich solcher, die ausschließlich für das technische Management berechtigt sind;

2. Weitergabekontrolle

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um zu verhindern, dass Personenbezogene Daten während ihrer Übertragung oder der Übermittlung des Datenträgers von nichtberechtigten Parteien gelesen, vervielfältigt, verändert oder gelöscht werden. Dies wird auf folgende Weise erreicht:

- Nutzung angemessener Firewall- und Verschlüsselungstechnologien;
- Soweit möglich, protokollierte und überwachte Übermittlung von Daten;

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit b DSGVO)

1. Verfügbarkeitskontrolle

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um sicherzustellen, dass Personenbezogene Daten vor zufälliger Zerstörung oder zufälligem Untergang geschützt sind. Dies wird auf folgende Weise erreicht:

- Redundanz der Infrastruktur um sicherzustellen, dass der Datenzugang innerhalb von sieben Tagen wiederhergestellt wird und zumindest einmal wöchentlich eine Datensicherung durchgeführt wird;
- Backups werden extern gelagert und sind verfügbar, falls die Infrastruktur für die Datenbankserver ausfällt;
- Regelmäßige Überprüfung von allen eingeführten und hier beschriebenen Sicherheitsmaßnahmen, zumindest alle sechs Monate;
- Backups werden nur erneut benutzt, wenn vorherige darauf enthaltene Informationen nicht verständlich sind und mit sämtlichen technischen Mitteln nicht rekonstruiert werden können;
- Andere Wechseldatenträger werden zerstört oder unbrauchbar gemacht, wenn sie nicht genutzt werden;
- Alle entdeckten Sicherheitsvorfälle werden aufgezeichnet, einschließlich der anschließenden Vorgänge zur Wiederherstellung der Daten und Identifizierung der ausführenden Person;

2. Belastbarkeit

Zeitnahes Wiederherstellen der Verfügbarkeit und des Zugangs zu Personenbezogenen Daten im Falle eines physischen oder technischen Vorfalls.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (Art. 32 Abs. 1 lit d DSGVO)

1. Datenschutzmanagement

Der Auftragsverarbeiter setzt ein geeignetes Datenschutzmanagement in seinem Unternehmen um.

2. Störfallmanagement

Der Auftragsverarbeiter setzt ein geeignetes Störfallmanagement um.

3. Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Der Auftragsverarbeiter setzt Datenschutz angemessen durch datenschutzfreundliche Voreinstellungen in seinem Unternehmen um.

4. Auftragskontrolle

Der Auftragsverarbeiter setzt geeignete Maßnahmen um, um sicherzustellen dass die Verarbeitung der Personenbezogenen Daten gemäß den Anweisungen des Verantwortlichen erfolgt. Dies wird auf folgende Weise erreicht:

- Schulung und Richtlinien für Arbeitnehmer des Auftragsverarbeiters; vorbehaltlich der Prüfung und Genehmigung des Datenexporteurs

Der Auftragsverarbeiter stellt sicher, dass wenn Sicherheitsmaßnahmen von externen Dritten erbracht werden, der Auftragsverarbeiter schriftliche Beschreibungen der ausgeführten Maßnahmen erhält, die eine Einhaltungen der Maßnahmen dieses Dokuments garantieren. Der Auftragsverarbeiter setzt außerdem geeignete Maßnahmen um, um seine Systemadministratoren zu überwachen und um sicherzustellen, dass sie in Übereinstimmung mit den erhaltenen Anweisungen handeln. Dies wird auf folgende Weise erreicht:

- Individuelle Ernennung der Systemadministratoren;
- Regelmäßige Audits der Aktivitäten der Systemadministratoren, um die Einhaltung der ihnen zugewiesenen Aufgaben, der Weisungen des Auftragsgebers und dem geltenden Recht zu prüfen; und
- Aufbewahren einer aktualisierten Liste mit den Identifikationsangaben der Systemadministratoren (z.B. Name, Nachname, Funktion oder Organisationsbereich) und zugewiesenen Aufgaben.

Anhang 3

Genehmigte Unterauftragsverabeiter

- **Host Europe GmbH**, Hansestrasse 111, 51149 Köln, Telefon: +49 2203 9934 1040, Telefax: +49 2203 9934 1042, E-Mail: info [at] hosteurope.de, Geschäftsführer Dr. Claus Boyens und Tobias Mohr.

  Auf den Servern der Host Europe GmbH findet die Datenverarbeitung aus Anhang 1 statt. Neben der Verarbeitung werden auch Backups aus der Datenverarbeitung bei Host Europe erstellt und gespeichert.

  Der Unterauftragsverarbeiter setzt geeignete Maßnahmen um, um zu verhindern, dass unberechtigte Personen Zutritt zu Datenverarbeitungsanlagen, mit deren Hilfe Personenbezogene Daten verarbeitet werden, erhalten. Diese Maßnahmen sind den TOMs von Host Europe aus der beiliegenden „Anlage_TOM_HostEurope“ zu entnehmen.

- **ialla.com UG** (haftungsbeschränkt), Am Weidenbach 25, 50259 Pulheim, Tel: 02238-465565, Mobil: 0173-3165220, e-Mail-Adressen, Info: info [at] ialla.com, Vertretungsberechtigter Geschäftsführer: Rainer Kittelmann.

  Der Unterauftragsverarbeiter setzt geeignete Maßnahmen um, um zu verhindern, dass unberechtigte Personen Zutritt zu Datenverarbeitungsanlagen, mit deren Hilfe Personenbezogene Daten verarbeitet werden, erhalten. Diese Maßnahmen sind den TOMs von ialla.com aus der beiliegenden „Anlage_TOM_ialla“ zu entnehmen.