Vertrag über die Verarbeitung von personenbezogenen Daten im Auftrag (Auftragsverarbeitungsvertrag)

Zwischen

mediacode solutions S.à r.l.
40-42 Grand Rue
6630 Wasserbillig
Luxembourg

- nachfolgend bezeichnet als "**Auftragsverarbeiter**" -

und

Ihr Firmenname + Anschrift

- nachfolgend bezeichnet als "**Auftraggeber**" -

- beide nachfolgend als "**die Vertragsparteien**" bezeichnet -

Alle Begrifflichkeiten verstehen sich geschlechtsneutral.

wird der folgende Auftragsverarbeitungsvertrag geschlossen:

Präambel und Anwendungsbereich

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftragsverarbeitungsvertrag konkretisiert die Auftragsverarbeitung im Hinblick auf ihren Gegenstand und den sich aus dem Auftragsverarbeitungsverhältnis ergebenden Ansprüche und Pflichten zwischen den Vertragsparteien.

Der Auftragsverarbeitungsvertrag findet keine Anwendung, wenn die DSGVO auf die Verarbeitung von personenbezogenen Daten durch den Auftraggeber nicht anwendbar ist (zum Beispiel bei ausschließlich persönlichen oder familiären Tätigkeiten entsprechend Art. 2 Abs. 2 lit. c. DSGVO) und der Auftragsverarbeiter daher nicht als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO handelt.

1. Begrifflichkeiten und Definitionen

a. "Auftragsverarbeitung" - Als "Auftragsverarbeitung" ist, im Einklang mit Art. 4 Nr. 8 DSGVO, die im Auftrag des Verantwortlichen, unabhängig von der Zahl dazwischen geschalteter Auftragsverarbeiter, durch den Auftragsverarbeiter entsprechend dem Gegenstand dieses Auftragsverarbeitungsvertrages eine Verarbeitung personenbezogener Daten gem. Art. 4 Nr. 2 DSGVO zu verstehen.

b. "Hauptvertrag" - Der Begriff des Hauptvertrages umfasst alle Arten laufender Geschäftsbeziehungen zwischen dem Auftraggeber und dem Auftragsverarbeiter, in deren Rahmen der Auftragsverarbeiter personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers entsprechend den Angaben zum Gegenstand der Auftragsverarbeitung in diesem Auftragsverarbeitungsvertrag verarbeitet. Sofern die Geltung dieses Auftragsverarbeitungsvertrages anderweitig (d. h. innerhalb dieser Vereinbarung oder außerhalb, in anderen Verträgen oder Regelungen) auf bestimmte Arten, Typen oder konkrete Geschäftsbeziehungen, Verträge, etc. beschränkt wurde, sind diese jeweils als Hauptvertrag zu verstehen. Der Begriff des Hauptvertrages umfasst auch laufende Einzelaufträge des Auftraggebers an den Auftragsverarbeiter, die von dem Auftraggeber im Rahmen des Hauptvertrages erteilt werden (z. B. im Fall von Rahmenverträgen).

c. "Verantwortlicher" - "Verantwortlicher" ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO).

d. „Personenbezogene Daten" - "Personenbezogene Daten" (nachfolgend auch

kurz als "Daten" bezeichnet) sind im Einklang mit Art. 4 Nr. 1 DSGVO 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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

e. "Betroffene Personen" - Als betroffene Personen (kurz "Betroffene") werden entsprechend Art. 4 Nr. 1 DSGVO Personen bezeichnet, die mittels von personenbezogenen Daten zumindest identifizierbar sind. Die von dieser Auftragsverarbeitung betroffenen Personen, ergeben sich aus dem Gegenstand der Auftragsverarbeitung.

f. "Dritte" - „Dritte" sind entsprechend Art. 4 Nr. 10 DSGVO natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

g. "Unterauftragsverarbeitung" - Wenn ein Auftragsverarbeiter nicht direkt vom Verantwortlichen beauftragt wurde, sondern von einem Auftragsverarbeiter des Verantwortlichen, liegt eine "Unterauftragsverarbeitung" vor und die dem ersten Auftragsverarbeiter folgenden Auftragsverarbeiter, werden als "Unterauftragsverarbeiter" bezeichnet.

h. "Elektronisches Format" - Erklärungen gelten als im "elektronischen Format" entsprechend Art. 28 Abs. 9 DSGVO abgegeben, wenn die erklärende Person erkennbar ist und das elektronische Erklärungsformat sich zum Nachweis der Erklärung eignet. Als "elektronisches Format" werden insbesondere die Textform, eine auf dauerhaften Datenträgern gespeicherte Vereinbarung (z. B. E-Mail), digitale Signierverfahren oder Verwendung dedizierter Onlinefunktionen (z. B. in Benutzerkonten) verstanden.

2. Art der Auftragsverarbeitung

a. Der Auftraggeber ist Verantwortlicher der Auftragsverarbeitung und im Rahmen dieses Auftragsverarbeitungsvertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung sowie für die Rechtmäßigkeit der Beauftragung des Auftragsverarbeiters verantwortlich. Der Auftraggeber ist

allein verantwortlich für die Erfüllung seiner Informationspflichten gegenüber betroffenen Personen gemäß Art. 13/14 DSGVO und stellt sicher, dass die Nutzung der durch den Auftragnehmer bereitgestellten Dienste in seinen Datenschutzerklärungen zutreffend dargestellt wird.

b. Im Rahmen der Betrugserkennung können IP-Adressen über Dienste von IT-Sicherheits- und Betrugspräventionsanbietern geprüft werden, die als eigene Verantwortliche tätig sind.

3. Weisungsbefugnis

a. Der Auftragsverarbeiter darf personenbezogene Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten und nur insoweit die Verarbeitung im Rahmen des Hauptvertrages erforderlich ist.

b. Mündliche Weisungen können erfolgen, wenn sie aufgrund der Umstände (z. B. Eilbedürftigkeit) geboten sind und sind unverzüglich schriftlich oder in elektronischer Form zu bestätigen.

c. Ist der Auftragsverarbeiter aufgrund objektiver Umstände der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird der Auftragsverarbeiter den Auftraggeber unverzüglich darauf hinweisen und die Ansicht sachlich begründen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung bis zur ausdrücklichen Bestätigung der Weisung durch den Auftraggeber auszusetzen und offensichtlich rechtswidrige Weisungen abzulehnen.

d. Der Auftragsverarbeiter kann Weisungen ablehnen, sofern deren Erfüllung dem Auftragsverarbeiter nicht möglich oder nicht zuzumuten ist (insbesondere, weil deren Befolgung ein unverhältnismäßiger Aufwand oder fehlende technische Möglichkeiten entgegenstehen). Die Ablehnung kann nur unter sachgerechter Berücksichtigung des Schutzes der Daten der betroffenen Personen erfolgen und berechtigt den Auftraggeber zur außerordentlichen Kündigung des Auftragsverarbeitungsvertrages, wenn dessen Fortsetzung dem Auftraggeber nicht zuzumuten ist.

e. Der Auftragsverarbeiter hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

4. Technische- und organisatorische Maßnahmen (Sicherheits- und Schutzkonzept)

1. Der Auftragsverarbeiter wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „TOMs") zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung, insbesondere durch regelmäßige Evaluation sicherstellen. Zu den TOMs gehören im Hinblick auf den Schutz der personenbezogenen Daten insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Integritäts- und Verfügbarkeitskontrolle, Trennungskontrolle sowie die Sicherung der Betroffenenrechte.
2. Die bei Vertragsschluss durch den Auftragsverarbeiter mitgeteilten TOMs definieren das vom Auftragsverarbeiter geschuldete Minimum des Sicherheitsniveaus. Die TOMs dürfen entsprechend dem technischen und rechtlichen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.
3. Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung der Daten befassten Mitarbeitern, Beauftragten und anderen für den Auftragsverarbeiter tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisung zu verarbeiten. Der Auftragsverarbeiter stellt ferner sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen in die gesetzlichen sowie sich aus diesem Auftragsverarbeitungsvertrag ergebenden Datenschutzbestimmungen eingewiesen und auf Vertraulichkeit und Verschwiegenheit verpflichtet worden sind oder einer entsprechenden und angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragsverarbeiter trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen regelmäßig angemessen angeleitet und überwacht werden.
4. Die Verarbeitung der personenbezogenen Daten außerhalb der Betriebsstätte des Auftragsverarbeiters (z. B. im Home- oder Mobileoffice oder bei Fernzugriff) ist zulässig, sofern die erforderlichen technischen und organisatorischen Maßnahmen ergriffen und dokumentiert werden, die den Besonderheiten dieser Verarbeitungssituationen in angemessener Weise Rechnung tragen und insbesondere auch eine ausreichende Kontrolle der Datenverarbeitung ermöglichen (z. B. Abschluss einer Vereinbarung über Datenschutz im Home- und Mobile-Office

mit Mitarbeitern).

5. Die im Auftrag durchgeführten Verarbeitungsprozesse werden vom Auftragsverarbeiter in einem angemessenen Umfang, in einem Verzeichnis von Verarbeitungstätigkeiten auf Anfrage in geeigneter Form nachweisbar dokumentiert und dem Auftraggeber auf Anforderung bereitgestellt.
6. Der Auftragsverarbeiter hat den Nachweis, einer im Rahmen dieses Auftragsverarbeitungsvertrages ordnungsgemäß erfolgten Vernichtung, bzw. Löschung von Daten und Dateien im angemessenen Umfang zu führen und auf Anfrage dem Auftraggeber zur Verfügung zu stellen.

    a. Sofern durch gesetzliche Vorgaben erforderlich, benennt der Auftragsverarbeiter eine den gesetzlichen Anforderungen entsprechende Datenschutzbeauftragte Person. Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktinformationen der Datenschutzbeauftragten sowie spätere Änderungen mit.

    b. Die im Rahmen des Auftragsverarbeitungsvertrag überlassene Daten sowie Datenträger und sämtliche hiervon gefertigten Kopien, verbleiben im Eigentum, bzw. in Inhaberschaft des Auftraggebers, unterliegen der Verfügungsherrschaft des Auftraggebers, sind durch den Auftragsverarbeiter sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers vernichtet werden. Die Vernichtung hat datenschutzgerecht und so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich und nicht zu erwarten ist. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragsverarbeiters gegenüber dem Auftraggeber erforderlich sind (z. B. Backups) und das vertragliche sowie das gesetzliche Datenschutzniveau gewährleistet werden.

    c. Der Auftragsverarbeiter ist verpflichtet, eine nach diesem Auftragsverarbeitungsvertrag unverzüglich herbeizuführende Rückgabe bzw. Löschung der Daten und Datenträger auch bei Unterauftragsverarbeitern herbeizuführen.

    d. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftragsverarbeiters oder den gesetzlichen Anforderungen nicht oder nicht mehr genügen, benachrichtigt der Auftragsverarbeiter den Auftraggeber unverzüglich.

5. Informationspflichten und Mitwirkungspflichten des Auftragsverarbeiters

a. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Auftraggeber oder im Fall zwingender gesetzlicher Pflichten, gerichtlicher oder gesetzlicher Informationen erteilen. Wendet sich eine betroffene Person an den Auftragsverarbeiter und macht ihre Betroffenenrechte geltend (insbesondere Rechte auf Auskunft oder Berichtigung, bzw. Löschung personenbezogener Daten), wird der Auftragsverarbeiter die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter und unterstützt den Auftraggeber im Rahmen der Zumutbarkeit und Möglichkeit. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird, soweit dies nicht von dem Auftragsverarbeiter zu vertreten ist.

b. Der Auftragsverarbeiter hat den Auftraggeber unverzüglich und vollständig zu informieren, wenn der Auftragsverarbeiter im Hinblick auf die Verarbeitung der personenbezogenen Daten Fehler oder Unregelmäßigkeiten bei der Einhaltung von Bestimmungen dieses Auftragsverarbeitungsvertrages und/ oder einschlägiger Datenschutzvorschriften feststellt. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der personenbezogenen Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

c. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragsverarbeiter tätig wird und deren Tätigkeit die für den Auftraggeber verarbeiteten Daten betreffen kann. Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunfts- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden.

d. Sollte die Sicherheit der personenbezogenen Daten des Auftraggebers durch Maßnahmen Dritter (z. B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird der Auftragsverarbeiter die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z. B. Widersprüche, Anträge, etc. stellen).

e. Der Auftragsverarbeiter stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im Rahmen dieses Auftragsverarbeitungsvertrages, die für die Erfüllung von gesetzlichen Pflichten des Auftraggebers (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung seiner Rechenschaftspflichten einer Datenschutz-Folgenabschätzung gehören können) notwendig sind, zur Verfügung und unterstützt diesen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

f. Die Informationspflichten des Auftragsverarbeiters erstrecken sich zunächst auf Informationen, die dem Auftragsverarbeiter, seinen Beschäftigten und Beauftragten vorliegen. Die Informationen müssen nicht von dritten Quellen beschafft werden, wenn die Beschaffung durch den Auftraggeber im zumutbaren Rahmen erfolgen könnte und keine anderweitige Vereinbarung getroffen wurde.

g. Der Auftragsverarbeiter muss Einhaltung seiner sich aus der Auftragsverarbeitung ergebenden vertraglichen und gesetzlichen Pflichten jederzeit mit geeigneten Mitteln nachweisen können.

6. Maßnahmen bei Gefährdung oder Verletzung des Datenschutzes

7. Die Information über eine (mögliche) Verletzung des Schutzes personenbezogener Daten hat unverzüglich, grundsätzlich innerhalb von 72 Stunden ab Kenntniserlangung zu erfolgen.

    a. Für den Fall, dass der Auftragsverarbeiter Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten personenbezogenen Daten im Sinne des Art. 4 Nr. 12 DSGVO verletzt sein könnte, hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten, insbesondere im Zusammenhang mit der Meldung an zuständige Behörden oder betroffene Personen zu unterstützen.

    b. Die Meldung des Auftragsverarbeiters muss entsprechend Art. 33 Abs. 3 DSGVO, mindestens die folgenden Angaben beinhalten:

        a. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der betroffenen Kategorien von Daten und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

        b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder

einer sonstigen Anlauf- oder Kontaktstelle für weitere Informationen;

c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (z. B. unter Angabe weiterer Details: Identitätsdiebstahl, Vermögensnachteile, etc.);

d. eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

c. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen oder von ihm Beauftragten gegen datenschutzrechtliche Bestimmungen oder die in diesem Auftragsverarbeitungsvertrag getroffenen Festlegungen.

7. Überprüfungen und Inspektionen

8. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses Auftragsverarbeitungsvertrag, insbesondere der TOMs beim Auftragsverarbeiter im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren und die erforderlichen Überprüfungen, einschließlich Inspektionen, durchzuführen.

   a. Der Auftragsverarbeiter hat den Auftraggeber bei den Kontrollen und Inspektionen im erforderlichen Rahmen zu unterstützen (z. B. durch Bereitstellung von Personal und Gewährung von Zugangs- und Zugriffsrechten).

   b. Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage) anzumelden. In Notfällen, d. h., wenn ein Zuwarten die Rechte der Betroffenen und/oder des Auftraggebers für diese in einem nicht zumutbaren Maße gefährden würde, kann eine angemessen kürzere Frist gewählt werden. Umgekehrt kann eine längere Frist erforderlich sein (wenn z. B. umfangreiche Vorbereitungen erfolgen müssen oder während der Urlaubszeit). Die Abweichungen von der Frist sind jeweils von der sie in Anspruch nehmenden Vertragspartei zu begründen.

   c. Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie den Schutz von personenbezogenen Daten Dritter (z. B. anderer Kunden oder

Mitarbeiter des Auftragsverarbeiters) Rücksicht nehmen. Vermeidbare Betriebsstörungen sind zu vermeiden. Soweit dem Anlass und Zweck der Prüfung genügend, soll sich eine Kontrolle auf Stichproben beschränken.

d. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie interne Prozesse des Auftragsverarbeiters und personenbezogene Daten zur Vertraulichkeit- und Verschwiegenheit verpflichtet sind. Der Auftragsverarbeiter kann den Nachweis einer entsprechenden Verpflichtung verlangen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen oder sonst ein begründeter Anlass zur seiner Ablehnung vorliegen, hat der Auftragsverarbeiter gegen diesen ein Einspruchsrecht.

e. Statt der Einsichtnahmen und der Vor-Ort-Kontrollen, darf der Auftragsverarbeiter den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte (z. B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Dies gilt nur, wenn der Verweis dem Auftraggeber zuzumuten ist und die Art sowie Umfang der Prüfung und Verweise der Art und dem Umfang des berechtigten Kontrollvorhabens des Auftraggebers entsprechen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

f. Der Auftraggeber übt sein Kontrollrecht grundsätzlich nicht häufiger als alle 12 Monate aus, es sei denn ein konkreter Anlass (insbesondere eine Verletzung des Datenschutzes, ein Sicherheitsvorfall oder das Ergebnis einer Auditierung) macht Kontrollen vor Ablauf dieses Zeitraums erforderlich.

8. Unterauftragsverhältnisse

a. Der Auftraggeber erklärt sich unbeschadet etwaiger Einschränkungen durch den Hauptvertrag ausdrücklich damit einverstanden, dass der Auftragsverarbeiter im Rahmen der Auftragsverarbeitung Unterauftragsverarbeiter einsetzen darf. Der Auftragsverarbeiter informiert den Auftraggeber mit einer angemessenen Vorfrist, die regelmäßig 14 Werktage beträgt, über neue Unterauftragsverarbeiter und gibt dem Auftraggeber die Möglichkeit die Unterauftragsverarbeiter vor deren Einsatz

im angemessenen Rahmen überprüfen und beim berechtigten Interesse Einspruch gegen den Einsatz der Unterauftragsverarbeiter erheben zu können. Erhebt der Auftraggeber keinen Einspruch innerhalb der Vorfrist, darf der Unterauftragsverarbeiter eingesetzt werden. Der Auftraggeber macht von seinem Recht auf Einspruch im Hinblick auf die Änderungen nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch.

b. Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters (z. B. eines Subunternehmers) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, dann muss er dem Unterauftragsverarbeiter im Wege eines Vertrags oder eines gesetzlich zulässigen anderen Rechtsinstruments im Wesentlichen dieselben datenschutzrechtlichen Pflichten, wie sie sich aus diesem Auftragsverarbeitungsvertrag ergeben. Die Pflichten können dabei auch durch allgemein verwendete Standardverträge, Standardvertragsklauseln der EU-Kommission oder im Markt übliche Auftragsverarbeitungsverträge des Unterauftragsverarbeiters erfüllt werden.

c. Der Auftragsverarbeiter wählt den Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung und der Zuverlässigkeit zur Einhaltung der Pflichten aus diesem Auftragsverarbeitungsvertrag sowie der Eignung der vom Unterauftragsverarbeiter getroffenen TOMs, sorgfältig aus.

d. Die Weiterleitung von im Auftrag verarbeiteten personenbezogenen Daten an Unterauftragsverarbeiter ist erst zulässig, wenn der Auftragsverarbeiter sich davon überzeugt hat, dass der Unterauftragsverarbeiter seine Verpflichtungen vollständig erfüllt hat. Die Prüfung ist auf Nachfrage in angemessener Form zu dokumentieren und die Dokumentation dem Auftraggeber auf Aufforderung vorzulegen.

e. Der Auftragsverarbeiter hat die Einhaltung der Pflichten der Unterauftragsverarbeiter, insbesondere der TOMs anlassbezogen, in einem angemessenen Umfang zu überprüfen. Die Prüfung und ihr Ergebnis sind so nachvollziehbar zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen. Statt eigener Überprüfung darf der Auftragsverarbeiter auf eine Überprüfung durch unabhängige Dritte (z. B. neutrale Datenschutzauditoren), Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise beim Subunternehmer unverzüglich zu unterrichten.

f. Die Verantwortlichkeiten zur Wahrnehmung der Pflichten aus diesem

Auftragsverarbeitungsvertrag und aus dem Gesetz sind zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter eindeutig zu regeln und voneinander abzugrenzen.

g. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragsverarbeiter gegenüber dem Auftraggeber.

h. Verarbeitungen von personenbezogenen Daten, die keinen direkten Zusammenhang mit der Erbringung der Hauptleistung aus dem Hauptvertrag aufweisen und bei denen der Auftragsverarbeiter die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt um seine geschäftliche Tätigkeit auszuüben (z. B. Reinigungs-, Bewachungs-, Wartungs-, Telekommunikations- oder Transportleistungen) stellen keine Unterauftragsverarbeitung im Sinne der vorstehenden Regelungen dieses Auftragsverarbeitungsvertrages dar. Gleichwohl hat der Auftragsverarbeiter sicher zu stellen, z. B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses Auftragsverarbeitungsvertrages und der Datenschutzvorschriften eingehalten werden.

i. Unterauftragsverhältnisse, die dem Auftraggeber bei Abschluss dieses Auftragsverarbeitungsvertrages mitgeteilt wurden, gelten in dem mitgeteilten Umfang unter Geltung der Regelungen dieses Auftragsverarbeitungsvertrages zu Unterauftragsverhältnissen als genehmigt.

j. Die bereits zum Abschluss dieses Auftragsverarbeitungsvertrages bestehenden Unterauftragsverhältnisse, werden vom Auftragsverarbeiter im **Anhang „Unterauftragsverhältnisse"** aufgeführt und durch den Auftragsverarbeiter aktualisiert.

k. Einsatz eigenständiger Dienstleister im Bereich IT-Sicherheit und Betrugsprävention

Der Auftragsverarbeiter kann zur Erbringung der vertraglich geschuldeten Leistungen Drittanbieter aus dem Bereich IT-Sicherheit und Betrugsprävention einsetzen. Diese Drittanbieter verarbeiten insbesondere IP-Adressen zur Erkennung von missbräuchlicher oder betrügerischer Nutzung (z. B. Proxy-/VPN- oder Missbrauchsmuster). Diese Drittanbieter handeln als eigene Verantwortliche im Sinne der DSGVO und nicht als Unterauftragsverarbeiter des Auftragnehmers. Der Auftragnehmer übermittelt an diese Drittanbieter nur die hierfür erforderlichen Daten und nur, soweit dies zur Erbringung der Betrugserkennungs- und Schutzfunktionen erforderlich ist. Der Auftraggeber bleibt dafür

verantwortlich, die Nutzung solcher Drittanbieter sowie die entsprechende Datenübermittlung in seinen eigenen Datenschutzhinweisen gegenüber betroffenen Personen transparent zu machen.

9. Räumlicher Bereich der Auftragsverarbeitung

a. Die Verarbeitung darf in Drittstaaten erfolgen, sofern die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, d. h. insbesondere a) die EU-Kommission ein angemessenes Datenschutzniveau festgestellt hat; b) auf Grundlage von wirksamen Standardschutzklauseln (sog. Standard Contractual Clauses, SCC); oder c) auf Grundlage von anerkannten verbindlichen internen Datenschutzvorschriften.

b. Die Genehmigung von Unterauftragsverhältnissen durch den Auftraggeber im Rahmen dieses Auftragsverarbeitungsvertrages, erstreckt sich auch auf den räumlichen Bereich der Auftragsverarbeitung.

c. Die Auftragsverarbeitung in einem anderen, als den vorstehend genannten Ländern, auch durch Unterauftragsverarbeiter, bedarf der vorherigen Genehmigung des Auftraggebers.

10. Pflichten des Auftraggebers

a. Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen, Weisungen oder Verarbeitungsprozessen Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen feststellt.

b. Die Auftraggeber benennt die zum Empfang von Weisungen berechtigte Ansprechpartner und ist verpflichtet Änderungen der Ansprechpartner oder deren Kontaktinformationen sowie Vertreter im Fall einer nicht vorübergehenden Abwesenheit oder Verhinderung unverzüglich mitzuteilen.

c. Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch betroffene Personen, dritte Unternehmen, Stellen oder Behörden hinsichtlich etwaiger Ansprüche aufgrund der Verarbeitung von personenbezogenen Daten im Rahmen dieses Auftragsverarbeitungsvertrages, verpflichtet sich der Auftraggeber den Auftragsverarbeiter bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten und unter Berücksichtigung des Verschuldensgrades der Vertragsparteien zu unterstützen.

11. Haftung

9. Die nachfolgenden Regelungen betreffen ausschließlich das Innenverhältnis zwischen Auftraggeber und Auftragsverarbeiter. Zwingende gesetzliche Ansprüche betroffener Personen, insbesondere nach Art. 82 DSGVO, werden hierdurch nicht beschränkt. Im Innenverhältnis zwischen den Parteien ist die Haftung des Auftragsverarbeiters für Fälle einfacher Fahrlässigkeit – gleich aus welchem Rechtsgrund – pro Schadensfall der Höhe nach auf das Sechsfache der vom Auftraggeber geschuldeten monatlichen Entgelte für die vom Schaden betroffene Leistung begrenzt („Haftungshöchstbetrag pro Schadensfall"). Darüber hinaus ist die Haftung des Auftragsverarbeiters aus und im Zusammenhang mit diesem Vertrag für Fälle einfacher Fahrlässigkeit insgesamt auf das Zwölffache der vom Auftraggeber geschuldeten monatlichen Entgelte für die vom Schaden betroffene Leistung pro Vertragsjahr begrenzt („Haftungshöchstbetrag pro Vertragsjahr"). Maßgeblich ist jeweils das vertraglich vereinbarte durchschnittliche monatliche Nettoentgelt für die konkret betroffene Leistung im Zeitpunkt des schadensauslösenden Ereignisses. Besteht der Vertrag zum Zeitpunkt des schadensauslösenden Ereignisses noch keine zwölf (12) Monate, so ist der Durchschnitt der bis dahin angefallenen monatlichen Entgelte zugrunde zu legen. Soweit gesetzlich zulässig, haftet der Auftragsverarbeiter nicht für mittelbare Schäden, Folgeschäden, entgangenen Gewinn sowie Schäden aus Betriebsunterbrechungen; etwaig dennoch zu ersetzende derartige Schäden unterliegen ausschließlich den vorstehenden Haftungshöchstbeträgen. Die Haftung des Auftragsverarbeiters für von Aufsichtsbehörden verhängte Geldbußen, sonstige öffentlich-rechtliche Sanktionen sowie für vom Auftraggeber gegenüber Dritten übernommene Vertragsstrafen ist ausgeschlossen, es sei denn, der Auftragsverarbeiter hat den haftungsbegründenden Verstoß vorsätzlich oder grob fahrlässig verursacht; in diesem Fall gelten die gesetzlichen Regelungen. Die vorstehenden Haftungsbegrenzungen gelten nicht für Schäden, die der Auftragsverarbeiter oder seine gesetzlichen Vertreter oder Erfüllungsgehilfen vorsätzlich oder grob fahrlässig verursacht haben, sowie nicht für Schäden aus der Verletzung von Leben, Körper oder Gesundheit.

   Es gelten die gesetzlichen Haftungsregelungen, insbesondere Art. 82 DSGVO sowie im Falle des Einsatzes eines Unterauftragsverarbeiters Art. 28 Abs. 4. S. 2 DSGVO.

12. Laufzeit und Fortgeltung nach Vertragsende

a. Dieser Auftragsverarbeitungsvertrag wird mit dessen Unterzeichnung, bzw. Abschluss in einem elektronischen Format wirksam.

b. Laufzeit und Ende dieses Auftragsverarbeitungsvertrages richten sich nach der Laufzeit und dem Ende des Hauptvertrages.

c. Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Pflichten und Vorgaben dieses Auftragsverarbeitungsvertrages und des geltenden Datenschutzrechts. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragsverarbeiter die in dem Auftragsverarbeitungsvertrag bestimmten Pflichten und die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

d. Der außerordentlichen Kündigung hat bei unerheblichen Pflichtverstößen eine Abmahnung der Verstöße mit angemessener Frist zur Abhilfe vorauszugehen, wobei die Abmahnung nicht erforderlich ist, wenn nicht damit zu rechnen ist, dass die beanstandeten Verstöße behoben werden oder diese derart schwer wiegen, dass ein Festhalten am Auftragsverarbeitungsvertrag der kündigenden Vertragspartei nicht zuzumuten ist.

e. Die Kündigung dieses Auftragsverarbeitungsvertrages, als auch die Aufhebung dieser Formklausel müssen zumindest im elektronischen Format erfolgen.

f. Die sich aus dem Auftragsverarbeitungsvertrag ergebenden Pflichten zum Schutz vertraulicher Informationen gelten auch nach Ende des Auftragsverarbeitungsvertrages fort, sofern der Auftragsverarbeiter weiterhin die vom Auftragsverarbeitungsvertrag umfassten personenbezogenen Daten verarbeitet und die Einhaltung der Pflichten für den Auftragsverarbeiter auch nach Vertragsende zumutbar ist.

13. Löschung und Herausgabe von Daten

10. Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses Auftragsverarbeitungsvertrages, wird der Auftragsverarbeiter alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl des Auftraggebers entweder vernichten oder zurückgeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. In diesem Fall informiert der Auftragsverarbeiter den Auftraggeber über die Verpflichtung und deren Umfang, es sei denn dass die Kenntnis der Verpflichtung seitens des Auftraggebers erwartet werden kann. Die Vernichtung, bzw. Löschung hat datenschutzgerecht und so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich und nicht zu erwarten ist. Die Einrede eines Zurückbehaltungsrechts wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick

auf die Löschung oder Rückgabe, gelten die Auskunfts-, Nachweis und Kontrollrechte des Auftraggebers entsprechend diesem Auftragsverarbeitungsvertrag.

11. Die Löschung und Vernichtung personenbezogener Daten hat durch den Auftragsverarbeiter datenschutzkonform und nach dem Stand der Technik zu erfolgen. Soweit Datenträger zu vernichten sind, hat die Vernichtung mindestens nach DIN 66399 Teile 1–3 unter Anwendung der vom Auftraggeber festgelegten Schutzklasse und mindestens der Sicherheitsstufe 4 in der jeweils einschlägigen Materialklasse zu erfolgen. Ist eine sofortige Löschung personenbezogener Daten auf Sicherungskopien aufgrund der besonderen Art der Speicherung nur mit unverhältnismäßig hohem Aufwand möglich, sind die betroffenen Daten nach Abstimmung mit dem Auftraggeber unverzüglich für jede weitere Verarbeitung einzuschränken und spätestens mit dem nächsten regulären Lösch- oder Überschreibungszyklus endgültig zu löschen.

12. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auch nach Beendigung des Auftragsverarbeitungsverhältnisses alle Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der Pflichten zur Löschung, Vernichtung oder Herausgabe personenbezogener Daten gegenüber Aufsichtsbehörden, Gerichten oder betroffenen Personen nachzuweisen. Der Auftraggeber ist berechtigt, die ordnungsgemäße Durchführung der in diesem Abschnitt geregelten Maßnahmen innerhalb eines Zeitraums von drei Jahren nach Vertragsende zu überprüfen oder überprüfen zu lassen; der Auftragsverarbeiter hat hierbei in angemessenem Umfang mitzuwirken.

13. Soweit der Auftragsverarbeiter personenbezogene Daten aufgrund zwingender gesetzlicher Aufbewahrungspflichten über das Ende des Auftragsverarbeitungsverhältnisses hinaus speichern muss, hat er den Auftraggeber hierüber unverzüglich in Textform zu informieren und Art sowie Umfang der jeweiligen Aufbewahrungspflicht darzulegen. Die betroffenen personenbezogenen Daten sind für jede weitere Verarbeitung zu sperren und dürfen ausschließlich zu dem Zweck der Erfüllung der gesetzlichen Aufbewahrungspflicht verarbeitet werden. Nach Wegfall der Aufbewahrungspflicht sind die betreffenden personenbezogenen Daten unverzüglich nach Maßgabe dieses Abschnitts zu löschen oder zu vernichten und der Löschvorgang entsprechend zu dokumentieren und nachzuweisen.

14. Die Einrede eines Zurückbehaltungsrechts wird hinsichtlich sämtlicher im Rahmen des Auftragsverarbeitungsverhältnisses verarbeiteten personenbezogenen Daten sowie der zugehörigen Datenträger ausgeschlossen. Dies gilt unabhängig von etwaigen offenen Forderungen oder sonstigen Ansprüchen des Auftragsverarbeiters gegenüber dem Auftraggeber.

14. Aufwandsentschädigung

a. Zusätzliche Aufwände bei der Unterstützung des Auftraggebers bei der Erfüllung seiner datenschutzrechtlichen oder anderer Pflichten werden angemessen vergütet mit den Stundensätzen, die im Dienstleistungsvertrag festgelegt sind.

b. Die nach dem Auftragsverarbeitungsvertrag vereinbarte Aufwandsentschädigung oder Vergütung umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragsverarbeiter beanspruchten Personals sowie erforderliche Auslagen (z. B. Reise- oder Materialkosten). Sofern möglich, absehbar und zumutbar, teilt der Auftragsverarbeiter dem Auftraggeber die Höhe der Aufwandsentschädigung oder Vergütung im Wege einer sachgerechten Schätzung vor deren Entstehung mit.

c. Überschreitet der mit den Weisungen des Auftraggebers einhergehende Aufwand für den Auftragsverarbeiter einen nach dem Hauptvertrag vereinbarten oder sonst branchenüblich zu erwartenden Rahmen und der Auftragsverarbeiter trägt kein Verschulden hieran, hat der Auftraggeber dem Auftragsverarbeiter den entstehenden Mehraufwand gesondert zu vergüten.

d. Überschreitet der mit der Zurverfügungstellung von Informationen und/ oder die erforderlichen Mitwirkung des Auftragsverarbeiters einhergehende Aufwand für den Auftragsverarbeiter einen nach dem Hauptvertrag vereinbarten oder sonst branchenüblich zu erwartenden Rahmen und der Auftragsverarbeiter trägt kein Verschulden hieran, hat der Auftraggeber dem Auftragsverarbeiter den entstehenden Mehraufwand gesondert zu vergüten.

e. Überschreitet der mit der Duldung und Mitwirkung bei den Kontrollen, bzw. adäquaten Alternativmaßnahmen einhergehende Aufwand für den Auftragsverarbeiter einen nach dem Hauptvertrag vereinbarten oder sonst branchenüblich zu erwartenden Rahmen und der Auftragsverarbeiter trägt kein Verschulden hieran, hat der Auftraggeber dem Auftragsverarbeiter den entstehenden Mehraufwand gesondert zu vergüten.

f. Überschreitet der mit der Löschung, bzw. der Rückgabe der Daten einhergehende Aufwand für den Auftragsverarbeiter einen nach dem Hauptvertrag vereinbarten oder sonst branchenüblich zu erwartenden Rahmen und der Auftragsverarbeiter trägt kein Verschulden hieran, hat der Auftraggeber dem Auftragsverarbeiter den entstehenden Mehraufwand gesondert zu vergüten.

15. Schlussbestimmungen

a. Das anwendbare Recht bestimmt sich nach dem Hauptvertrag.

b. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist der (Wohn)Sitz des Auftragsverarbeiters und sofern vom geltenden Gesetz zwingend vorgesehen, der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder wenn der Auftraggeber im Geltungsbereich des anwendbaren Rechts keinen Gerichtsstand hat. Der Auftragsverarbeiter behält sich vor, Ansprüche an dem gesetzlichen Gerichtsstand geltend zu machen.

c. Der vorliegende Auftragsverarbeitungsvertrag stellt die vollständige, zwischen den Vertragsparteien getroffene Vereinbarung dar. Nebenabreden bestehen nicht.

d. Mit Zustandekommen dieses Auftragsverarbeitungsvertrages werden alle etwaigen früheren Verträge aufgehoben, die zwischen den Vertragsparteien dieses Vertrages abgeschlossen wurden und die die Verarbeitung personenbezogener Daten im Auftrag regeln, wenn und soweit diese den gleichen Gegenstand der Auftragsverarbeitung betreffen und wenn und soweit zwischen den Vertragsparteien nicht ausdrücklich schriftlich etwas anderes vereinbart wurde.

e. Änderungen sowie Ergänzungen dieses Auftragsverarbeitungsvertrages, als auch die Aufhebung dieser Formklausel müssen zumindest im elektronischen Format erfolgen.

f. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz den Regelungen des Hauptvertrages vor.

g. Sollten eine oder mehrere Bestimmungen dieses Auftragsverarbeitungsvertrages unwirksam oder undurchführbar sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die unwirksamen Bestimmungen werden vielmehr im Wege der ergänzenden Auslegung eine solche Regelung ersetzt, die von den Vertragsparteien mit der/den unwirksamen Bestimmung/en erkennbar verfolgten wirtschaftlichen Zweck möglichst nahekommt. Sofern die vorbenannte ergänzende Auslegung aufgrund gesetzlich zwingender Vorgaben nicht möglich ist, werden die Vertragsparteien eine ihr entsprechende Regelung vereinbaren.

Der Auftragsverarbeitungsvertrag wird im elektronischen Format abgeschlossen und ist ohne Unterschriften der Vertragsparteien wirksam.

16. Anhang: Gegenstand der Auftragsverarbeitung

Die folgenden Angaben zur Art und zum Zweck der Verarbeitung, der Art der personenbezogenen Daten sowie den Kategorien betroffener Personen, bestimmen den Gegenstand der durch den Auftragsverarbeitungsvertrag geregelten Verarbeitung. Änderungen des Gegenstandes der Verarbeitung und weiterer Verfahrensänderungen sind zwischen den Vertragsparteien gemeinsam abzustimmen und zu dokumentieren.

Personenbezogene Daten des Auftraggebers werden auf Grundlage dieses Auftragsverarbeitungsvertrages zu den folgenden Zwecken verarbeitet:

a. Der Auftragnehmer setzt unterstützende KI-Dienste (z. B. Large Language Models) zur Analyse von IP- und Fingerprint-Daten ein, um Anomalien und potenziell betrügerisches Verhalten zu identifizieren. Die KI-Auswertung dient als Bestandteil eines technischen Regelwerks, welches automatisiert zur Einstufung einer IP-Adresse als unverdächtig oder verdächtig beitragen kann. Die Verarbeitung erfolgt nicht als Hochrisiko-KI gemäß EU-KI-Verordnung; es werden keine Entscheidungen mit rechtlicher Wirkung für betroffene Personen im Sinne des Art. 22 DSGVO getroffen. Automatisierte Entscheidungen dienen ausschließlich der IT-Sicherheit und betrugspräventiven Werbesteuerung. Eine unmittelbare Rechtswirkung oder erhebliche Beeinträchtigung für betroffene Personen liegt nicht vor.

b. Zur Betrugsprävention und Erkennung missbräuchlicher oder betrügerischer Nutzung (z. B. ungültiger Traffic, wiederkehrende Fake-Anfragen, Proxy-/VPN-Missbrauch) können IP-Adressen über spezialisierte Dienstleister aus dem Bereich IT-Sicherheit und Betrugsprävention geprüft werden, die als eigene Verantwortliche tätig sind.

c. Beratungsleistungen.

d. Erbringung von Leistungen im Bereich der IT-Sicherheit.

e. Kundenmanagement und / oder Kundensupport.

f. Software-as-Service-Leistungen (SaaS).

g. Leistungen im Bereich der Softwareerstellung und-/ oder Wartung.

h. Web- und Cloud-Hosting.

i. Werbung und Marketing (Beratung, Konzeption, Umsetzung und Durchführung).

Zu den auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Arten

und Kategorien von personenbezogenen Daten gehören:

a. Nutzungsdaten.

b. Standortdaten.

c. Protokolldaten.

d. Meta- und Verbindungsdaten.

e. Telemetriedaten.

Zu den durch die Verarbeitung von personenbezogenen Daten auf Grundlage dieses Auftragsverarbeitungsvertrages betroffenen Personengruppen gehören:

a. Webseitenbesucher.

b. Softwarenutzer.

Die auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Daten werden aus den im Folgenden genannten Quellen, bzw. im Rahmen genannter Verfahren erhoben oder sonst empfangen:

a. Erhebung bei betroffenen Personen.

b. Erhebung im Rahmen der Nutzung von Software, Applikationen, Webseiten und anderen Onlinediensten.

c. Erhebung über Schnittstellen zu Diensten anderer Anbieter.

d. Externe Datenbanken und Datensammlungen.

e. Empfang im Wege der Übermittlung oder sonstiger Mitteilung durch oder im Auftrag des Auftraggebers.

Anhang: Technisch-organisatorische Maßnahmen (TOMs)

Es wird für die konkrete Verarbeitung und die in ihrem Rahmen verarbeiteten personenbezogenen Daten ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau Gewähr geleistet. Dazu werden insbesondere die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Organisatorische Maßnahmen

Es sind organisatorische Maßnahmen ergriffen worden, die ein angemessenes Datenschutzniveau und dessen Aufrechterhaltung gewährleisten.

a. Eine geeignete Organisationsstruktur für die Datensicherheit und Datenschutz ist vorhanden und die Informationssicherheit ist integriert in unternehmensweite Prozesse und Verfahren integriert.

b. Es sind interne Sicherheitsricht- bzw. -leitlinien definiert, die unternehmensintern gegenüber Mittarbeitern als verbindliche Regeln kommuniziert werden.

c. Die Entwicklung des Standes der Technik sowie aktuelle Bedrohungen und Sicherheitsmaßnahmen werden fortlaufend beobachtet. Die daraus gewonnenen Erkenntnisse fließen in geeigneter Weise in die Weiterentwicklung des eigenen Sicherheitskonzepts ein.

d. Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden (Wartungs-, Wach-, Transport- und Reinigungsdienste, freie Mitarbeiter, etc.), werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten. Sofern die Dienstleister im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten des Auftraggebers erhalten oder sonst das Risiko eines Zugriffs auf die personenbezogenen Daten besteht, werden sie speziell auf Verschwiegenheit und Vertraulichkeit verpflichtet.

e. Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung

verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt.

f. Eingesetzte Software und Hardware wird stets auf dem aktuell verfügbaren Stand gehalten und Softwareaktualisierungen werden ohne Verzug innerhalb einer angesichts des Risikograd es und eines eventuellen Prüfnotwendigkeit angemessenen Frist ausgeführt. Es wird keine Software und Hardware eingesetzt, die von den Anbietern im Hinblick auf Belange des Datenschutzes- und Datensicherheit nicht mehr aktualisiert wird (z. B. abgelaufene Betriebssysteme).

g. Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen.

h. Unterlagen im Papierformat werden nur dann aufbewahrt, wenn keine im Hinblick auf die Auftragsverarbeitung, ihrem Zweck und den Interessen der von den Inhalten der Unterlagen betroffenen Personen adäquate digitale Kopie vorliegt oder eine Aufbewahrung mit dem Auftraggeber vereinbart wurde oder gesetzlich erforderlich ist.

i. Die Verarbeitung der Daten des Auftraggebers, die nicht entsprechend den Vereinbarungen dieses Auftragsverarbeitungsvertrages gelöscht wurden (z. B. in Folge der gesetzlichen Archivierungspflichten), wird im erforderlichen Umfang durch Sperrvermerke und/oder Aussonderung eingeschränkt.

Zugangskontrolle

Es sind Maßnahmen zur elektronischen Zugangskontrolle ergriffen worden, die gewährleisten, dass ein Zugang (d. h. bereits die Möglichkeit der Nutzung, Verwendung oder Beobachtung) durch Unbefugte zu Systemen, Datenverarbeitungsanlagen oder Verfahren verhindert wird.

a. Ein Passwortkonzept legt fest, dass Passwörter eine dem Stand der Technik und den Anforderungen an Sicherheit entsprechende Mindestlänge und Komplexität haben müssen.

b. Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.

c. Passwörter werden grundsätzlich nicht im Klartext gespeichert und nur gehashed oder verschlüsselt übertragen.

d. Zugangsdaten werden, wenn deren Benutzer das Unternehmen oder Organisation des Auftragsverarbeiters verlassen haben, gelöscht oder deaktiviert.

e. Es wird auf dem aktuellen Stand gehaltene Anti-Viren-Software eingesetzt.

f. Einsatz von Hardware-Firewall(s).

g. Einsatz von Software-Firewall(s).

Interne Zugriffskontrolle und Eingabekontrolle (Berechtigungen für Benutzerrechte auf Zugang zu und Änderung von Daten)

Es sind Maßnahmen zur Zugriffskontrolle ergriffen worden, 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 nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ferner sind Maßnahmen zur Eingabekontrolle ergriffen worden, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert, entfernt oder sonst verarbeitet worden sind.

a. Ein Rechte- und Rollenkonzept (Berechtigungskonzept) sorgt dafür, dass der Zugriff auf personenbezogenen Daten nur für einen nach Erforderlichkeitsmaßstäben ausgewählten Personenkreis und nur in dem erforderlichen Umfang möglich ist.

b. Die Tätigkeiten der Administratoren werden im Rahmen rechtlich zulässiger Möglichkeiten und im Rahmen technisch vertretbaren Aufwandes angemessen überwacht und protokolliert.

c. Es wird sichergestellt, dass nachvollziehbar ist, welche Beschäftigten oder Beauftragten auf welche Daten wann Zugriff hatten (z. B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).

Weitergabekontrolle

Es sind Maßnahmen zur Weitergabekontrolle ergriffen worden, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Die Übermittlung und Verarbeitung von personenbezogenen Daten des Auftraggebers über Onlineangebote (Webseiten, Apps, etc.), erfolgt geschützt mittels einer TLS oder einer gleichwertig sicheren Verschlüsselung.

Auftragskontrolle, Zweckbindung und Trennungskontrolle

Es sind Maßnahmen zur Auftragskontrolle ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Die Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten des Auftraggebers getrennt verarbeitet werden und keine Vermengung, Verschnitt oder sonstige dem Auftrag widersprechende gemeinsame Verarbeitung dieser Daten erfolgt.

a. Die für den Auftraggeber durchgeführten Verarbeitungsprozesse werden in einem angemessenen Umfang, in einem Verzeichnis von Verarbeitungstätigkeiten gesondert dokumentiert.

b. Sorgfältige Auswahl von Unterauftragsverarbeitern und sonstigen Dienstleistern.

c. Die für die Verarbeitung der personenbezogenen Daten des Auftraggebers geltenden Löschfristen werden innerhalb des Löschkonzepts des Auftragsverarbeiters, sofern erforderlich gesondert, dokumentiert.

Sicherung der Integrität und Verfügbarkeit von Daten sowie der Belastbarkeit von

Verarbeitungssystemen

Es sind Maßnahmen ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und in Notfällen zügig wiederhergestellt werden können.

a. Es werden ausfallsichere Serversysteme und Dienste eingesetzt, die doppelt, bzw. mehrfach ausgelegt sind.

b. Die personenbezogenen Daten werden bei externen Hosting-Anbietern gespeichert. Die Hosting-Anbieter werden sorgfältig ausgewählt und erfüllen die Vorgaben an den Stand der Technik, im Hinblick den Schutz vor Schäden durch Brand, Feuchtigkeit, Stromausfälle, Katastrophen, unerlaubte Zugriffe sowie an Datensicherung und Patchmanagement, als auch an die Gebäudesicherung.

c. Die zur Verarbeitung eingesetzten Serversysteme verfügen über eine unterbrechungsfreie Stromversorgung (USV), die gegen Ausfälle angemessen gesichert ist und ein geregeltes Herunterfahren in Notfällen ohne Datenverlust sicherstellt.

d. Die zur Verarbeitung eingesetzten Serversysteme verfügen über einen angemessenen Brandschutz (Feuer- und Rauchmeldeanlagen sowie entsprechende Feuerlöschvorrichtungen oder Feuerlöschgeräte).

e. Es werden Serversysteme eingesetzt, die über einen Schutz vor Feuchtigkeitsschaden (z. B. Feuchtigkeitsmelder) verfügen.

Anhang: Unterauftragsverarbeiter

Der Auftragsverarbeiter setzt die folgenden Unterauftragsverarbeiter im Rahmen der Verarbeitung von Daten für den Auftraggeber ein:

- **Microsoft Azure:** Leistungen auf dem Gebiet der Bereitstellung von informationstechnischer Infrastruktur und verbundenen Dienstleistungen (z. B. Speicherplatz und/oder Rechenkapazitäten); **Dienstanbieter:** Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland; **Website:** https://azure.microsoft.com; **Datenschutzerklärung:** https://privacy.microsoft.com/de-de/privacystatement. **Auftragsverarbeitungsvertrag:** https://azure.microsoft.com/de-de/support/legal/.
- **Roboro S.à r.l.:** Dienstleistungen im Bereich der technischen Administration, Wartung und Verwaltung von Cloud-Infrastrukturen in Microsoft Azure.
  Der Dienstleister hat im Rahmen der Systemadministration potenziellen Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers in der Azure-Umgebung verarbeitet werden.
  Die Verarbeitung erfolgt ausschließlich auf Weisung des Auftragnehmers.
  Rechtsgrundlage: Auftragsverarbeitung gemäß Art. 28 DSGVO.
  Es besteht ein zwischen den Parteien abgeschlossener Auftragsverarbeitungsvertrag; **Dienstanbieter:** Roboro S.à r.l.
  40-42 Grand Rue
  L-6630 Wasserbillig; **Website:** https://www.roboro.lu.
  Datenschutzerklärung: https://www.roboro.lu/datenschutzerklaerung/.
- **Sentry:** Überwachung der Systemstabilität und Ermittlung von Codefehlern - Angaben zum Gerät oder Fehlerzeitpunkt werden pseudonym erhoben und werden anschließend gelöscht; **Dienstanbieter:** Functional Software Inc., Sentry, 132 Hawthorne Street, San Francisco, California 94107, USA; **Website:** https://sentry.io; **Sicherheitsmaßnahmen:** IP-Masking (Pseudonymisierung der IP-Adresse); **Datenschutzerklärung:** https://sentry.io/privacy/. **Auftragsverarbeitungsvertrag:** https://sentry.io/legal/dpa/.
- **Hetzner:** Leistungen auf dem Gebiet der Bereitstellung von informationstechnischer Infrastruktur und verbundenen Dienstleistungen (z. B. Speicherplatz und/oder Rechenkapazitäten); **Dienstanbieter:** Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland; **Website:** https://www.hetzner.com; **Datenschutzerklärung:** https://docs.hetzner.com/de/general/company-and-policy/data-protection-at-hetzner. **Auftragsverarbeitungsvertrag:**

https://docs.hetzner.com/de/general/company-and-policy/data-protection-at-hetzner.