Dienstleistungsrahmenvertrag

zwischen

– ***Auftraggeber*** *(definiert per Angebotsannahme)* –

und

PREDICTA|ME GmbH

Pfarrgasse 20

55268 Nieder-Olm

– *nachfolgend Auftragnehmer genannt* –

wird folgender Dienstleistungsrahmenvertrag geschlossen:

§ 1 Vertragsgegenstand

(1) Vorliegend handelt es sich um einen Rahmenvertrag. Die konkrete Beauftragung (Einzelauftrag) erfolgt durch die Bestätigung eines individuellen Angebots oder durch einen separaten, schriftlichen Auftrag durch den Auftraggeber.

(2) Der Auftraggeber beabsichtigt, dem Auftragnehmer Aufträge im Bereich folgender Dienstleistungen zu erteilen:

- Mitarbeitersuche durch Dienstleistungsverfahren von PREDICTA|ME und Partnern auf Basis eines Anforderungsprofils des Auftraggebers
- Analyse von Kompetenzmerkmalen von Mitarbeitern/Bewerbern
- Erstellung von Team- und/oder Organisationsanalysen (Stimmung, Engagement, Risiken)
- Analyse und Identifizierung der stellenspezifischen oder situationsspezifischen Anforderungsprofile für die Passungsanalysen
- Erstellung von vergleichenden Analysen zwischen Bewerber- und/oder Mitarbeiterprofilen und den Anforderungsprofilen des Auftraggebers
- Set-Up und Durchführung von unternehmensspezifischen Puls- und/oder Mitarbeiterumfragen

- Set-Up und Durchführung von unternehmensspezifischen 180°/270°/360° Feedback Analysen

§ 2 Leistungen des Auftragnehmers

Zur Erfüllung der in § 1 genannten Aufgaben wird der Auftragnehmer insbesondere folgende Leistungen erbringen (bezieht sich immer nur auf ein konkret vorliegendes Angebot):

- Kandidatensuche durch Dienstleistungsverfahren
- Spezifische Erstellung von Mitarbeiterumfragen nach den Erfordernissen des Auftraggebers
- Datenauswertung der erhobenen Daten durch PREDICTA|ME Puls- und/oder Mitarbeiterumfragen
- Datenauswertung und Reporting der erhobenen Daten durch PREDICTA|ME Analysen zur Erstellung von Kompetenzprofilen oder einem „competence fitting“

§ 3 Vergütung

(1) Der Auftragnehmer erhält vom Auftraggeber eine Vergütung, die in einem jeweils individuellen Angebot festgelegt wird.

(2) Die Vergütung ist jeweils 14 Tage nach Rechnungsstellung fällig.

(3) Außergewöhnliche Dienstleistungen, insbesondere die individuelle Erstellung umfangreicher Mitarbeiterumfragen, werden nach vorheriger Vereinbarung zwischen den Parteien gesondert vergütet.

§ 4 Vertragsdauer

Dieses Vertragsverhältnis beginnt mit Unterzeichnung des Vertrages und läuft auf unbestimmte Zeit. Das Vertragsverhältnis ist von beiden Seiten schriftlich kündbar mit einer Frist von 4 Wochen. Das beiderseitige Recht zur vorzeitigen außerordentlichen – auch fristlosen – Kündigung, bleibt unberührt.

§ 5 Mitwirkungspflicht des Auftraggebers

(1) Der Auftraggeber hat dafür Sorge zu tragen, dass dem Auftragnehmer alle für die Ausführung seiner Tätigkeit notwendigen Unterlagen rechtzeitig vorgelegt werden, ihm alle Informationen erteilt werden und er von allen Vorgängen und Umständen in Kenntnis gesetzt wird. Dies gilt auch für Unterlagen, Vorgänge und Umstände, die erst während der Tätigkeit des Auftragnehmers bekannt werden.

(2) Auf Verlangen des Auftragnehmers hat der Auftraggeber die Richtigkeit und Vollständigkeit der von ihm vorgelegten Unterlagen sowie seiner Auskünfte und mündlichen Erklärungen schriftlich zu bestätigen

(3) Es gelten die AGB des Auftragnehmers unter https://www.predictame.de/agb

§ 6 Haftung

(1) Der Auftragnehmer haftet nur für vorsätzliche oder grob fahrlässig verschuldete Verletzungen des Vertrages. Die Beweislast des Verschuldens liegt beim Auftraggeber. Die Haftung des Auftragnehmers für Folgeschäden, reine Vermögensschäden, entgangener Gewinn, Zinsverlust und von Schäden aus Ansprüchen Dritter ist ausgeschlossen. Der Auftragnehmer übernimmt keinerlei Haftung für nicht termingerechte Auslieferung, Übersendung oder Anmeldung von Daten aufgrund technischer Störungen unabhängig von deren Verursacher.

(2) Der Auftragnehmer übernimmt keine Haftung für die Umsetzung der Testergebnisse.

(3) Der Auftragnehmer haftet nicht für verloren gegangene, beschädigte und unvollständig erhaltene Postsendungen oder E-Mails. Auch für rechtzeitig abgesendete Postsendungen und E-Mails, die trotzdem nicht termingerecht ankommen, wird – unabhängig vom Verursacher – keine Haftung übernommen. Daraus resultierende Folgeschäden werden nicht anerkannt.

§ 7 Schweigepflicht, Datenschutz

(1) Der Auftragnehmer ist verpflichtet, über alle Informationen, die ihm im Zusammenhang mit seiner Tätigkeit für den Auftraggeber bekannt werden, Stillschweigen zu bewahren, gleichviel ob es sich dabei um den Auftraggeber selbst oder dessen Geschäftsverbindungen handelt, es sei denn, dass der Auftraggeber ihn von dieser Schweigepflicht entbindet.

(2) Der Auftragnehmer ist befugt, ihm anvertraute personenbezogene Daten im Rahmen seiner Tätigkeit zu verarbeiten oder verarbeiten zu lassen. Umgang, Art und Zweck der Erhebung, Nutzung und Verarbeitung von Daten durch den Auftragnehmer sind diesem Vertrag als Anlage 1, 2 und 3 beigefügten und sind ein wesentlicher Bestandteil des Vertrages. Bei Einschaltung Dritter hat der Auftragnehmer deren Verpflichtung zur Verschwiegenheit sicherzustellen.

§ 8 Aufbewahrung und Rückgabe von Unterlagen

Der Auftragnehmer verpflichtet sich, alle ihm zur Verfügung gestellten Geschäfts- und Betriebsunterlagen ordnungsgemäß aufzubewahren, insbesondere dafür zu sorgen, dass Dritte nicht Einsicht nehmen können. Die zur Verfügung gestellten Unterlagen sind während der Dauer des Vertrages auf Anforderung, nach Beendigung des Vertrages unaufgefordert dem Vertragspartner zurückzugeben oder zu löschen.

§ 9 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform.

(2) Mündliche Nebenabreden bestehen nicht.

(3) Sind oder werden einzelne Bestimmungen dieses Vertrages unwirksam, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die Vertragspartner werden in diesem Fall die ungültige Bestimmung durch eine andere ersetzen, die dem wirtschaftlichen Zweck der weggefallenen Regelung in zulässiger Weise am nächsten kommt.

(4) Ausschließlicher Gerichtsstand für sämtliche Rechtstreitigkeiten zwischen den Parteien aus und im Zusammenhang mit diesem Dienstleistungsvertrag oder seinen Anlagen ist der Sitz des Auftragnehmers.

Anlagen:

1 Auftragsdatenverarbeitung

2 Konkretisierung der Auftragsverarbeitung

3 Technische und organisatorische Maßnahmen

Anlage 1 Auftragsdatenverarbeitung

Präambel

Der Auftraggeber beauftragt den Auftragnehmer mit der Durchführung von Online-Analysen zur Personalsuche und/oder Passungsdiagnostik und/oder zur Persönlichkeitsentwicklung und/oder zur Teamentwicklung und/oder mit der Durchführung von Puls- und/oder Mitarbeiterumfragen. Der Zweck der Datenspeicherung und -verarbeitung besteht darin, Mitarbeiter im Auftrag zu finden und/oder psychologische Test- und Fragebogenverfahren zur Personalauswahl und -entwicklung durchzuführen. Die Angabe personenbezogener Daten ist insbesondere zur eindeutigen Identifikation der Teilnehmer, zur Vorbeugung von Missbrauch sowie zur Kommunikation mit den Teilnehmern erforderlich. Um die Rechte und Pflichten aus dem Auftragsverhältnis gemäß den gesetzlichen Verpflichtungen zu konkretisieren, schließen die Vertragsparteien folgende Vereinbarung:

Soweit der Auftragnehmer im Rahmen seiner o.g. Tätigkeiten im Unternehmen des Auftraggebers Zugriff auf personenbezogene Daten sowie sonstige vertrauliche Informationen oder Betriebsgeheimnisse des Auftraggebers erhält, so haben er und seine eingesetzten Mitarbeiter diese Daten und Informationen strikt vertraulich zu behandeln. Personenbezogene Daten sind Angaben jedweder Art zu einer bestimmten oder bestimmbaren natürlichen Person, gleichgültig ob Mitarbeiter oder Kunde bzw. Lieferant. Auch Daten ohne direkten Personenbezug (z. B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen geschlossen werden kann (z. B. Personalnummer, PC-Benutzerkennung). Vertrauliche Informationen im Sinne dieser Erklärung sind alle mündlichen oder schriftlichen Informationen, Daten, Unterlagen, Materialen und Angaben, die der Auftragnehmer direkt oder indirekt vom Auftraggeber zur Abwicklung des Auftrages erhält oder in die er im Rahmen seiner Tätigkeiten Einsicht erhält. Dies gilt insbesondere, wenn diese Unterlagen, Materialien oder Informationen als vertraulich gekennzeichnet sind oder deren Vertraulichkeit sich aus ihrem Gegenstand oder sonstigen Umständen ergibt. Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen finden daher Anwendung auf alle Leistungen der Auftragsverarbeitung, die der Auftragnehmer gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

1. Gegenstand und Dauer des Auftrags

a) Der Gegenstand der Nutzung ergibt sich aus den vom Auftraggeber bestellten Leistungen und ist in Anlage 2 „Konkretisierung der Auftragsverarbeitung“ zu dieser Vereinbarung niedergelegt.

b) Die Dauer dieser Vereinbarung tritt mit Unterzeichnung beider Parteien in Kraft. Sie endet mit der Beendigung der Erhebung, Verarbeitung und/oder Nutzung der Daten des Auftraggebers,

sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen des Auftragnehmers ergeben.

2. Konkretisierung des Auftragsinhalts

a) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers sind in Anlage 2 beschrieben.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sowie in der Schweiz statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

b) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

X Adressdaten	X Kontaktdaten	X Abrechnungsdaten
X Leistungsdaten	X Finanzdaten	X Angebotsdaten
X Gesprächshistorie	X Transaktionsdaten	X Auskünfte
X Mitarbeiterdaten	X Personalverwaltung	X Qualifikationsdaten
X Videoaufzeichnungen	X Vertragsdaten	

☐ Sonstige:

c) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

X Mitarbeiter	X Ruheständler	X Bewerber
X Praktikanten	X Frühere Mitarbeiter	X Kunden
X Interessenten	X Lieferanten/Dienstleister	X Berater
X Kontaktpersonen	X Auszubildende	

☐ Sonstige:

3. Technische und organisatorische Maßnahmen

a) Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

b) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Einzelheiten sind in Anlage 2 beschrieben.

c) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

d) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42 a BDSG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42 a BDSG zu unterstützen.

4. Berichtigung, Einschränkung und Löschung von Daten

a) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

b) Zu einem vom Auftraggeber schriftlich festgelegten Zeitpunkt, jedoch spätestens 6 Monate nach Abschluss der vertraglichen Arbeiten, hat der Auftragnehmer sämtliche vom Auftraggeber übermittelten personenbezogenen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen zu löschen oder auszuhändigen.

c) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

d) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

e) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragter ist beim Auftragnehmer Frau Dr. Yasmin Issa-Nummer bestellt:

Dr. Yasmin Issa-Nummer
PREDICTA|ME GmbH
Pfarrgasse 20
55268 Nieder-Olm
yasmin.issanummer@predictame.com

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 3).

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 der Anlage 1.

6. Unterauftragsverhältnisse

a) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

b) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO: Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

c) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Firma, Rechtsform	Anschrift	Beschreibung von Art und Umfang der Beauftragung
Strato AG Berlin	Pascalstraße 10 10587 Berlin	Rechenzentrum: Datenspeicherung und Verarbeitung
HELLO UMI S.L.	Calle Paris, 82 bajo 1 - Barcelona - 08029	Datenspeicherung und Verarbeitung Anbieter von Kommunikationsplattformen

d) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 1 (a) der Anlage 1 eingesetzt werden sollen.

e) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

a) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

b) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

c) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

d) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

a) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei

Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

I. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

II. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

III. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

IV. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

V. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

b) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

a) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

b) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Anlage 2: Konkretisierung der Auftragsverarbeitung

Der Auftragnehmer stellt über seine Websites www.predictame.de/www.predictame.com/www.predictport.com eine onlinebasierte Analyse- und Umfrageplattform zur Verfügung, über diese Passungs- und Kompetenzanalysen und Unternehmensumfragen durchgeführt und ausgewertet werden können.

Ergänzung zu Anlage 1, Ziffer 2 (a) Umfang, Art und Zweck der Datenverarbeitung:

Der Auftraggeber verwendet im folgenden Umfang und zum Zwecke des Feedbackmanagement die Online-Analyse des Auftragnehmers:

1. Durchführen von Kompetenzanalysen und/oder Umfragen und/oder Personalsuche
2. Einladen von Teilnehmern
3. Herunterladen von Analyseergebnissen und Ergebnisreports

Anlage 3: Technische und organisatorische Maßnahmen

Kontrollziele und Beschreibung der technischen und organisatorischen Maßnahmen im Rechenzentrum der Strato AG, nachfolgend „Rechenzentrum“ genannt, und der PREDICTA|ME GmbH, nachfolgend „PREDICTA|ME“ genannt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Kontrollziele bezüglich des Umgangs mit personenbezogenen Daten	Maßnahmen
1. Zutrittskontrolle (Räume und Gebäude) Zielbeschreibung: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.	Rechenzentrum: • Festlegung von Sicherheitsbereichen • Realisierung eines wirksamen Zutrittsschutzes • Festlegung zutrittsberechtigter Personen • Protokollierung des Zutritts • Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus • Begleitung von Besuchern und Fremdpersonal • Überwachung der Räume außerhalb der Betriebszeiten PREDICTA|ME GmbH: • Begleitung von Besuchern und Fremdpersonal
2. Zugangskontrolle (IT-Systeme, Anwendungen) Zielbeschreibung: Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.	Rechenzentrum: • Festlegung des Schutzbedarfs • Festlegung befugter Personen • Zugangsschutz (Authentisierung) • Umsetzung sicherer Zugangsverfahren, starke Authentisierung oder einfache Authentisierung je nach Schutzbedarf • Protokollierung des Zugangs • Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk • Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen • Automatische oder manuelle Zugangssperre • Durchführung von Datenkryptierungen bei Laptops PREDICTA|ME GmbH: • Zuordnung von Benutzerrechten • Authentifikation mit Benutzername / Passwort • Richtlinien für Kennwortvergabe: min. 8 Zeichen, min. 1 Großbuchstabe, min. 1 Sonderzeichen, min 1 Zahl • Alle 90 Tage Passwortwechsel • Protokollierung anhand von Log-Dateien • SSL-Verschlüsselung

3. Zugriffskontrolle (auf Daten) Zielbeschreibung: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen	Rechenzentrum: • Berechtigungskonzepte • Umsetzung von Zugriffsbeschränkungen • Vergabe minimaler Berechtigungen • Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen • Vermeidung der Konzentration von Funktionen PREDICTA|ME GmbH: • Berechtigungskonzept mit differenzierten Berechtigungen • SSL-Verschlüsselungsverfahren • Verwaltung der Rechte durch Systemadministrator • Anzahl der Administratoren auf das „Notwendigste“ reduziert • Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel • Einsatz von Aktenvernichtern • Alle befugten Personen, haben jeweils nur auf die für Sie relevanten Daten Zugriff und sind zur Einhaltung der datenschutzrechtlichen Gesetze und Regelungen verpflichtet und entsprechend geschult
4. Trennungskontrolle (zweckbezogen) Zielbeschreibung: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden	Rechenzentrum: • Vorhandensein von Richtlinien und Arbeitsanweisungen • Vorhandensein von Verfahrensdokumentation • Umsetzung von Regelungen zur Programmierung • Regelungen zur System- und Programmprüfung • Umsetzung eines Abstimm- und Kontrollsystems PREDICTA|ME GmbH: • Trennung von Datensätzen • Logische Mandantenfähigkeit (softwareseitig) • Erstellung eines Berechtigungskonzepts • Getrennte Test- und Produktionsumgebung

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Kontrollziele bezüglich des Umgangs mit personenbezogenen Daten	Maßnahmen
5. Weitergabekontrolle (von Daten) Zielbeschreibung: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur	Rechenzentrum: • Festlegung von empfangs-/weitergabeberechtigter Instanzen/Personen • Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland • Sichere Datenübertragung zwischen Server und Client • Risikominimierung durch Netzseparierung • Implementation von Sicherheitsgateways an den Netzübergabepunkten • Härtung der Backendsysteme • Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder • Umsetzung einer Maschine-Maschine-Authentisierung

	• Sichere Ablage von Daten inkl. Backups • Prozess zur Sammlung und Entsorgung • Einführung datenschutzgerechter Lösch- und Zerstörungsverfahren • Führung von Löschprotokollen PREDICTA|ME GmbH: • SSL Verschlüsselung der Datenübertragung auf Speichermedien • Schulung der betroffenen Personen zur Einhaltung und Verpflichtung der datenschutzrechtlichen Gesetze

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Kontrollziele bezüglich des Umgangs mit personenbezogenen Daten	Maßnahmen
6. Verfügbarkeitskontrolle (von Daten) Zielbeschreibung: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO).	Rechenzentrum: • Vorhandensein und Umsetzung eines Konzeptes zur Durchführung von regelmäßigen Datensicherungen • Vorhandensein und regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen • Überwachung der Betriebsparameter von Rechenzentren • Vorhandensein eines Notfallkonzeptes • Regelungen zur Aufnahme eines Krisen- bzw. Notfallmanagements PREDICTA|ME GmbH: • tägliches Backup 14-tägig rückwirkend • Firewall/Virenschutz

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs.1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Kontrollziele bezüglich des Umgangs mit personenbezogenen Daten	Maßnahmen
7. Auftragskontrolle Zielbeschreibung: Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	Rechenzentrum: • Protokollierung der Auftragsausführung durch den Auftragsverarbeiter PREDICTA|ME GmbH: • Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) • Schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag) • Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis nach §53 Bundesdatenschutzgesetz • Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten • Nachweis eines Datenschutz Management Systems nach EU DS-GVO