ALLGEMEINER AUFTRAGSVERARBEITUNGSVERTRAG

Artikel 28 Verordnung (EU) 2016/679 („DSGVO")

Zwischen

Dem Kunden, wie im Vertrag bestimmt („Verantwortlicher"), vertreten durch seinen mit den erforderlichen Befugnissen ausgestatteten gesetzlichen Vertreter, in seiner Eigenschaft als

Verantwortlicher

und

Dem Anbieter, wie im Kommerziellen Angebot und in Anlage A zu den Allgemeinen Bedingungen bestimmt, vertreten durch seinen mit den erforderlichen Befugnissen ausgestatteten gesetzlichen Vertreter („**Auftragsverarbeiter"** oder „**Anbieter**"), vertreten durch seinen mit den erforderlichen Befugnissen ausgestatteten gesetzlichen Vertreter, in seiner Eigenschaft als

Auftragsverarbeiter

Der Verantwortliche und der Auftragsverarbeiter werden nachstehend gemeinsam auch als „Parteien" und einzeln als „Partei" bezeichnet.

VORBEMERKUNGEN

I. die Parteien haben einen oder mehrere Verträge („Vertrag") über die Bereitstellung von Diensten („Dienste") unterzeichnet;

II. der Vertrag umfasst die Verarbeitung von Informationen, die gesetzlich als Personenbezogene Daten definiert sind, und die Parteien beabsichtigen daher, in diesem Allgemeinen Auftragsverarbeitungsvertrag („Auftragsverarbeitungsvertrag") die Bedingungen für die Verarbeitung Personenbezogener Daten zu regeln, die der Auftragsverarbeiter im Rahmen der Bereitstellung der Dienste gemäß dem Vertrag durchführt;

III. die Einzelheiten und spezifischen Merkmale oder besonderen Bedingungen der Verarbeitung Personenbezogener Daten sind in den sogenannten „Verarbeitungsblättern" zu einem oder mehreren vom Kunden aktivierten Diensten enthalten, die diesem Auftragsverarbeitungsvertrag jeweils beigefügt werden.

IV. Diese Verarbeitungsblätter beschreiben im Einzelnen die operativen Modalitäten der Verarbeitung in Bezug auf den jeweiligen Dienst und geben, soweit anwendbar, die Liste der Unterauftragsverarbeiter sowie etwaige angewandte zusätzliche Sicherheitsmaßnahmen an. Die Verarbeitungsblätter werden nach ihrer Unterzeichnung als weitere Anlagen in diesen Auftragsverarbeitungsvertrag aufgenommen und bilden deren integralen und wesentlichen Bestandteil;

V. bevor der Verantwortliche den Auftragsverarbeiter mit der Erbringung der Dienste betraut hat, hat er dessen Erfahrung, Fähigkeiten und Zuverlässigkeit geprüft und festgestellt, dass der Auftragsverarbeiter hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden und ein angemessener Schutz der verarbeiteten Daten und der Rechte der betroffenen Personen gewährleistet ist;

VI. der Auftragsverarbeiter hat die Verarbeitungsvorgänge gemäß den schriftlichen Weisungen des Verantwortlichen auf der Grundlage eines Vertrags oder eines anderen verbindlichen Rechtsinstruments durchzuführen, in dem Dauer, Art und Zwecke der Verarbeitung, die Kategorien der verarbeiteten Personenbezogenen Daten und der von der Verarbeitung betroffenen Personen sowie die Pflichten und Rechte des Auftragsverarbeiters in Bezug auf die Verarbeitung festgelegt sind;

VII. mit diesem Auftragsverarbeitungsvertrag beabsichtigt der Verantwortliche, den eingangs genannten Auftragsverarbeiter zum Auftragsverarbeiter zu bestellen und ihm alle erforderlichen Weisungen für die mit der Bereitstellung der Dienste verbundene Verarbeitung Personenbezogener Daten zu erteilen;

VIII. der Verantwortliche ermächtigt den Auftragsverarbeiter sowie die von diesem befugten Personen, ausschließlich auf die für die Ausführung des Vertrags unbedingt erforderlichen Personenbezogenen Daten („Personenbezogene Daten") zuzugreifen;

IX. dieser Auftragsverarbeitungsvertrag begründet keinen Anspruch des Auftragsverarbeiters auf besondere Vergütungen und/oder Entschädigungen und/oder Erstattungen, die über die gegebenenfalls bereits im Vertrag vorgesehenen hinausgehen, vorbehaltlich weiterer, ausdrücklich angeforderter und von den Parteien in einer gesonderten schriftlichen Vereinbarung vereinbarter Umsetzungen;

X. die tatsächliche Erbringung der Gegenstand des Vertrags bildenden Dienste kann für jeden Dienst durch eine bestimmte Gesellschaft der Namirial-Gruppe erfolgen, die in den jeweiligen Verarbeitungsblättern als „Erbringendes Unternehmen" bestimmt ist. Ist das Erbringende Unternehmen nicht mit dem Auftragsverarbeiter identisch, so wird es auf der Grundlage konzerninterner, mit Artikel 28 DSGVO konformer Vereinbarungen zwischen den Gesellschaften der Namirial-Gruppe tätig, die bereits vor und unabhängig von diesem Auftragsverarbeitungsvertrag bestehen; eine im jeweiligen Verarbeitungsblatt ausdrücklich festgelegte abweichende datenschutzrechtliche Rolle bleibt unberührt;

XI. handelt der Kunde als Auftragsverarbeiter im Auftrag eines anderen Verantwortlichen (der „Endkunde"), so übernimmt der Kunde in Bezug auf diese konkrete Verarbeitung gegenüber dem Anbieter die Pflichten und Verantwortlichkeiten eines Auftragsverarbeiters, wobei der Anbieter in diesem Zusammenhang die Rolle eines Unterauftragsverarbeiters übernimmt. In diesem Fall finden die Bestimmungen über die Datenverarbeitung und die Pflichten des Auftragsverarbeiters nach diesem Auftragsverarbeitungsvertrag Anwendung, jedoch mit der Maßgabe, dass der Kunde als Auftragsverarbeiter im Auftrag des Endkunden und der Auftragsverarbeiter als Unterauftragsverarbeiter im Auftrag des Kunden handelt;

XII. in jedem Fall, in dem der Kunde als Verantwortlicher oder als Auftragsverarbeiter im Auftrag des Endkunden handelt, erklärt sich der Auftragsverarbeiter bereit, die Rolle des Auftragsverarbeiters und/oder Unterauftragsverarbeiters wahrzunehmen, und verpflichtet sich daher, die Personenbezogenen Daten gemäß den vom Kunden erhaltenen Weisungen und so zu verarbeiten, dass der Schutz dieser Personenbezogenen Daten gemäß den in diesem Auftragsverarbeitungsvertrag und den ihm beigefügten Verarbeitungsblättern festgelegten Sicherheitsmaßnahmen gewährleistet ist.

DIES VORAUSGESCHICKT, VEREINBAREN DIE PARTEIEN WAS FOLGT

1. GELTUNG DER VORBEMERKUNGEN UND ANLAGEN. DEFINITIONEN

1.1. Die Vorbemerkungen und die Anlagen bilden einen integralen und wesentlichen Bestandteil dieses Auftragsverarbeitungsvertrags.

1.2. Sofern in diesem Auftragsverarbeitungsvertrag nichts anderes bestimmt ist, haben alle in diesem Auftragsverarbeitungsvertrag und in den Anlagen großgeschrieben verwendeten Begriffe die ihnen im Vertrag zugewiesene Bedeutung und gelten sowohl im Singular als auch im Plural. In Übereinstimmung mit den Begriffsbestimmungen des anwendbaren Rechts werden die Begriffe und Definitionen gemäß Anlage I – Definitionen zu diesem Auftragsverarbeitungsvertrag verwendet, auf die verwiesen wird.

1.3. Die Verarbeitungsblätter zu den vom Kunden genutzten Diensten können diesem Auftragsverarbeitungsvertrag auch zu einem späteren Zeitpunkt beitreten, wenn der Vertrag zur Aktivierung neuer Dienste ergänzt wird. In diesem Fall treten die von den Parteien zusammen mit dem Vertragsnachtrag unterzeichneten Anlagen dieses Auftragsverarbeitungsvertrags bei.

2. RECHTE UND PFLICHTEN DES VERANTWORTLICHEN

2.1. Der Verantwortliche überträgt dem Auftragsverarbeiter sämtliche – und ausschließlich die – Verarbeitungsvorgänge Personenbezogener Daten, die für die vollständige Ausführung des Vertrags erforderlich sind.

2.2. Der Verantwortliche erklärt, alle ihm nach dem Anwendbaren Datenschutzrecht obliegenden Pflichten in Bezug auf die Verarbeitung Personenbezogener Daten gemäß diesem Auftragsverarbeitungsvertrag zu erfüllen. Insbesondere:

a. hat der Verantwortliche das Recht und die Pflicht, die Entscheidungen über die Zwecke und Mittel der Verarbeitung zu treffen, einschließlich der Bestimmung der zutreffenden Rechtsgrundlage der Verarbeitung;
b. erklärt der Verantwortliche, dass die Personenbezogenen Daten den Zwecken, für die sie erhoben und anschließend verarbeitet werden, angemessen und erheblich sind, nicht darüber hinausgehen und unter Einhaltung sämtlicher Anforderungen des Anwendbaren Datenschutzrechts übermittelt werden;
c. erstellt der Verantwortliche angemessene und vollständige Informationen über die Verarbeitung Personenbezogener Daten gemäß Art. 13 und/oder Art. 14 DSGVO und stellt sie – soweit erforderlich – dem Auftragsverarbeiter zur Verfügung.

2.3. Der Verantwortliche verpflichtet sich, dem Auftragsverarbeiter jede in Bezug auf die Verarbeitungsvorgänge Personenbezogener Daten erforderliche Änderung förmlich mitzuteilen. Der Auftragsverarbeiter und seine Befugten Personen führen keine anderen als die vom Verantwortlichen gemäß diesem Artikel angegebenen Verarbeitungsvorgänge Personenbezogener Daten durch.

2.4. Der Verantwortliche gewährleistet, dass die gegebenenfalls vom Verantwortlichen und/oder von durch ihn beauftragten Dritten zur Verfügung gestellten Infrastrukturen und Systeme, auf denen der Auftragsverarbeiter die Verarbeitung durchzuführen hat („Systeme des Verantwortlichen"), geeignet sind, den einschlägigen Branchenstandards und -vorschriften entsprechen und die ordnungsgemäße Erbringung der Dienste im Einklang mit diesem Auftragsverarbeitungsvertrag ermöglichen. Der Verantwortliche verpflichtet sich daher, den Auftragsverarbeiter von jeglichen Störungen, Schäden oder Unterbrechungen bei der Durchführung der Verarbeitung freizustellen und schadlos zu halten, die sich aus der Ungeeignetheit, aus Anomalien und/oder etwaigen Fehlfunktionen der Systeme des Verantwortlichen ergeben, auf denen der Auftragsverarbeiter tätig werden muss.

3. PFLICHTEN DES AUFTRAGSVERARBEITERS

3.1. Im Rahmen seiner Zuständigkeiten aufgrund des Vertrags und diesem Auftragsverarbeitungsvertrag ist der Auftragsverarbeiter für sich und seine Befugten Personen verpflichtet, die Bestimmungen des Anwendbaren Datenschutzrechts einzuhalten, insbesondere die Bestimmungen der DSGVO und des Anwendbaren Datenschutzrechts sowie die anwendbaren Maßnahmen der zuständigen Aufsichtsbehörden, die Auftragsverarbeitern besondere Pflichten auferlegen;

3.2. Insbesondere führt der Auftragsverarbeiter die ihm übertragenen Verarbeitungsvorgänge gemäß den in diesem Auftragsverarbeitungsvertrag enthaltenen Weisungen des Verantwortlichen sowie gemäß etwaigen späteren Weisungen durch, die der Verantwortliche mit angemessener Vorankündigung schriftlich mitteilen kann.

3.3. Der Auftragsverarbeiter führt die für die ihm übertragenen Aufgaben erforderlichen Verarbeitungsvorgänge im Einklang mit diesem Auftragsverarbeitungsvertrag und mit den Zwecken durch, für die die Personenbezogenen Daten erhoben und verarbeitet werden. Eine von diesem Auftragsverarbeitungsvertrag abweichende Verarbeitung erfolgt nur auf dokumentierte Weisung des Verantwortlichen oder sofern der Auftragsverarbeiter nach dem Recht der Union oder der Mitgliedstaaten hierzu verpflichtet ist; in diesem Fall teilt der Auftragsverarbeiter dies dem Verantwortlichen vorab mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet.

3.4. Der Auftragsverarbeiter ist verpflichtet, die Dokumentation zu der ihm übertragenen Verarbeitung mittels geeigneter Verfahren nach Effizienzkriterien zu verwalten und die Aufbewahrung, Unverfälschtheit und leichte Auffindbarkeit sämtlicher für die Einhaltung der Anforderungen der DSGVO relevanten Dokumente zu gewährleisten.

3.5. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen und Dokumente zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen (Audits), einschließlich mit angemessener Vorankündigung mitgeteilter Inspektionen, die vom Verantwortlichen oder einem von diesem beauftragten Dritten gemäß den Bedingungen, Grenzen und Verfahren nach Artikel 10 durchgeführt werden, und trägt dazu bei.

3.6. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls eine Weisung seiner Auffassung nach gegen die DSGVO oder andere Bestimmungen des Anwendbaren Datenschutzrechts verstößt. Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen auf dessen Verlangen in Verfahren vor der

zuständigen Aufsichtsbehörde oder vor Gericht im Zusammenhang mit den in seine Zuständigkeit fallenden Verarbeitungstätigkeiten, insbesondere indem er alle Informationen und Dokumente zur Verfügung stellt, die zum Nachweis der Einhaltung der Pflichten nach dem Anwendbaren Datenschutzrecht in Bezug auf die Verarbeitung Personenbezogener Daten dienlich sind.

3.7. Der Auftragsverarbeiter informiert den Verantwortlichen über die Benachrichtigungs-E-Mail unverzüglich, spätestens jedoch innerhalb von 48 (achtundvierzig) Stunden, über jede Beanstandung, Inspektion oder rechtsverbindliche Anfrage einer Aufsichtsbehörde, eines Gerichts oder einer sonstigen Behörde, die die im Auftrag des Verantwortlichen verarbeiteten Personenbezogenen Daten betrifft. Im Falle eines Offenlegungsersuchens erfolgt die Information, bevor dem Ersuchen nachgekommen wird, und gibt, soweit rechtlich zulässig, die ersuchende Behörde, die Rechtsgrundlage, den Umfang des Ersuchens und die betroffenen Daten an. Der Auftragsverarbeiter kommt Ersuchen ohne rechtsverbindlichen Charakter nicht nach.

Die Information darf ausschließlich in dem Umfang und für den Zeitraum unterbleiben oder eingeschränkt werden, in dem das anwendbare Recht der Union oder der Mitgliedstaaten oder eine auf dessen Grundlage erlassene verbindliche Maßnahme sie aus wichtigen Gründen des öffentlichen Interesses untersagt. In diesem Fall dokumentiert der Auftragsverarbeiter das Verbot, legt nur die unbedingt erforderlichen Daten offen und informiert den Verantwortlichen, sobald das Verbot entfällt. Ersuchen von Behörden aus Drittländern werden auch nach Maßgabe von Artikel 48 und Kapitel V DSGVO geprüft.

3.8. Der Auftragsverarbeiter bestimmt innerhalb seiner Unternehmensorganisation die Befugten Personen, die zur Durchführung von Verarbeitungsvorgängen Personenbezogener Daten berechtigt sind. Gleichzeitig mit der Bestellung erteilt der Auftragsverarbeiter den Befugten Personen angemessene schriftliche Weisungen zu den Modalitäten der Verarbeitung gemäß Art. 29 DSGVO und diesem Auftragsverarbeitungsvertrag. Lediglich beispielhaft und nicht abschließend schreibt der Auftragsverarbeiter bei der schriftlichen Benennung der Befugten Personen vor, dass diese nur Zugang zu denjenigen Personenbezogenen Daten haben, deren Kenntnis für die Erfüllung der ihnen übertragenen Aufgaben unbedingt erforderlich ist (*need-to-know*-Prinzip). Der Auftragsverarbeiter hat ferner zu überprüfen, dass die Befugten Personen bei einer Verarbeitung mit elektronischen Mitteln sämtliche Sicherheitsmaßnahmen zur Verwahrung der Zugangsdaten anwenden. Der Auftragsverarbeiter überprüft zudem, dass die Befugten Personen nicht-elektronische Datenträger, die Kopien der Personenbezogenen Daten enthalten, insbesondere wenn diese Besonderen Kategorien angehören, sicher verwahren. Schließlich obliegt es dem Auftragsverarbeiter, die Befugten Personen in Bezug auf die von ihnen durchgeführten Verarbeitungsvorgänge Personenbezogener Daten wirksamen Vertraulichkeitspflichten zu unterwerfen, auch für den Zeitraum nach Beendigung des Beschäftigungsverhältnisses mit dem Auftragsverarbeiter.

3.9. Im Innenverhältnis zwischen den Parteien haftet der Auftragsverarbeiter für Schäden aus der Verarbeitung gemäß Art. 82 DSGVO nur insoweit, als diese Schäden durch einen ihm zurechenbaren Verstoß gegen die speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO oder dadurch verursacht wurden, dass er unter Nichtbeachtung oder gegen die rechtmäßig erteilten Weisungen des Verantwortlichen gehandelt hat. Die Haftung des Auftragsverarbeiters ist auf den Teil des Schadens beschränkt, der seinem tatsächlichen Verursachungsbeitrag entspricht, und unterliegt den im Vertrag vorgesehenen Haftungsbeschränkungen.

3.10. Soweit anwendbar und in dem Umfang, in dem es die für den jeweiligen Dienst oder das Erbringende Unternehmen geltenden Gesetze, Verordnungen oder verbindlichen Maßnahmen der zuständigen Aufsichtsbehörde verlangen, setzt der Auftragsverarbeiter geeignete Maßnahmen zur Identifizierung, Autorisierung, Unterweisung und Überwachung des Personals mit privilegierten oder administrativen Zugriffsrechten auf die für die Verarbeitung Personenbezogener Daten genutzten Systeme um. Etwaige länderspezifische Anforderungen, einschließlich der Anforderungen an Systemadministratoren, werden im jeweiligen Verarbeitungsblatt angegeben.

3.11. Gemäß Art. 28 Abs. 3 Buchst. a DSGVO nimmt der Verantwortliche in die Weisungen an den Auftragsverarbeiter die Durchführung von Verarbeitungen auf, die für die folgenden, der Verbesserung der Gegenstand des Vertrags bildenden Dienste dienenden Tätigkeiten unbedingt erforderlich sind: Test, Messung und Optimierung der Leistung, Kalibrierung und Validierung von Modellen/Algorithmen, Verbesserung von Genauigkeit/Zuverlässigkeit/Benutzerfreundlichkeit, Sicherheit und Betrugsprävention, Behebung von Fehlern (Bugs) und Anomalien, soweit diese der ordnungsgemäßen Erbringung der Dienste an den Verantwortlichen dienen. Jede Nutzung für eigenständige Zwecke des Auftragsverarbeiters oder seiner Unterauftragsverarbeiter, einschließlich Marketing, Profiling oder der Entwicklung nicht damit zusammenhängender Produkte/Dienste, ist ausgeschlossen.

3.12. Die Verbesserungstätigkeiten nach dem vorstehenden Absatz erfolgen nur in dem für die Erbringung, Wartung und Sicherheit der Dienste unbedingt erforderlichen Umfang oder auf Grundlage

anonymisierter/aggregierter Daten, vorbehaltlich abweichender Weisungen und vom Verantwortlichen gewählter Rechtsgrundlagen. Der Auftragsverarbeiter darf Unterauftragsverarbeiter einsetzen, sofern er ihnen das Verbot der Weiterverwendung der Daten und des Trainings von Modellen mit allgemeinem Verwendungszweck sowie die Pflicht zur Löschung der Daten nach Abschluss der Tätigkeiten auferlegt.

4. SICHERHEIT DER VERARBEITUNG

4.1. Im Rahmen seiner Zuständigkeit aufgrund des Vertrags und diesem Auftragsverarbeitungsvertrag ist der Auftragsverarbeiter für sich und die Befugten Personen verpflichtet, die nach dem Anwendbaren Datenschutzrecht vorgesehenen sowie die vom Verantwortlichen angegebenen Sicherheitsmaßnahmen umzusetzen und den Verantwortlichen bei der Gewährleistung der Einhaltung von Art. 32 DSGVO zu unterstützen.

4.2. Im Rahmen der mit der Bereitstellung der Dienste verbundenen Verarbeitungstätigkeiten Personenbezogener Daten verpflichtet sich der Anbieter, geeignete technische und organisatorische Maßnahmen zu treffen, um unrechtmäßige oder unbefugte Verarbeitungen zu verhindern und die Personenbezogenen Daten vor Vernichtung, Veränderung, Verlust, unbefugtem Zugang oder unbefugter Offenlegung zu schützen, wie in Anlage II – Technische und organisatorische Sicherheitsmaßnahmen zu diesem Auftragsverarbeitungsvertrag im Einzelnen beschrieben.

4.3. Anlage II beschreibt die vom Anbieter getroffenen Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie die Verfahren zur raschen Wiederherstellung des Zugangs zu den Personenbezogenen Daten bei einem Sicherheitsvorfall. Die umgesetzten Maßnahmen („Sicherheitsmaßnahmen") werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung im Verhältnis zum Risikoniveau der verarbeiteten Personenbezogenen Daten festgelegt. Der Kunde nimmt zur Kenntnis und akzeptiert, dass diese Maßnahmen geeignet sind, ein den anwendbaren regulatorischen Anforderungen entsprechendes Sicherheitsniveau zu gewährleisten; die Pflichten des Anbieters gemäß Art. 32 DSGVO bleiben unberührt.

4.4. Der Anbieter behält sich das Recht vor, die Sicherheitsmaßnahmen zu aktualisieren oder zu ändern, um eine fortlaufende Anpassung an technologische und regulatorische Entwicklungen zu gewährleisten, sofern solche Änderungen das Gesamtschutzniveau der Dienste nicht verringern.

4.5. Verlangt der Kunde die Einführung bestimmter zusätzlicher Sicherheitsmaßnahmen über die vorgesehenen hinaus, prüft der Anbieter die technische und betriebliche Durchführbarkeit dieser Anforderungen und behält sich vor, für etwaige Umsetzungen zusätzliche Kosten in Rechnung zu stellen.

4.6. Bei Produkten, die beim Kunden oder bei von ihm beauftragten Stellen installiert sind (z. B. On-Premises-Lösungen), gelten die vom Anbieter getroffenen Sicherheitsmaßnahmen ausschließlich für Dienste, die eine Verarbeitung Personenbezogener Daten durch den Anbieter oder seine Unterauftragsverarbeiter vorsehen (z. B. Fernsupport und -unterstützung oder Migrationsdienste).

4.7. Ermöglichen die Dienste die Integration mit Software oder Anwendungen Dritter, ist der Anbieter weder für die von diesen Dritten angewandten Sicherheitsmaßnahmen noch für etwaige Schwachstellen verantwortlich, die sich aus einer unmittelbar vom Kunden oder von Drittanbietern vorgenommenen Integration ergeben, es sei denn, die Integration wurde vom Anbieter bereitgestellt.

4.8. Unbeschadet der dem Anbieter obliegenden Sicherheitspflichten ist der Kunde dafür verantwortlich, alle erforderlichen Maßnahmen zu treffen, um den Schutz der Personenbezogenen Daten zu gewährleisten, die im Rahmen der Nutzung der Dienste durch sein Personal oder etwaige befugte Personen verarbeitet werden.

4.9. Der Kunde verpflichtet sich, die Dienste im Einklang mit den Sicherheits-Best-Practices zu nutzen und ein den mit der Verarbeitung Personenbezogener Daten verbundenen Risiken angemessenes Schutzniveau zu gewährleisten.

4.10. Der Kunde hat alle geeigneten Maßnahmen zum Schutz der Authentifizierungsdaten, der Geräte und der Systeme umzusetzen, die für den Zugang zu den Diensten genutzt werden, und regelmäßige Backups der Personenbezogenen Daten durchzuführen, um deren Wiederherstellung im Einklang mit den anwendbaren Vorschriften sicherzustellen, vorbehaltlich etwaiger ausdrücklich vereinbarter Backup- und Wiederherstellungspflichten des Anbieters.

4.11. Der Anbieter ist nicht verantwortlich für den Schutz Personenbezogener Daten, die der Kunde oder Dritte außerhalb der Systeme des Anbieters und seiner Unterauftragsverarbeiter verarbeiten, einschließlich Daten, die auf Papier oder in der internen IT-Infrastruktur des Kunden (z. B. private Rechenzentren oder On-Premises-Server) gespeichert sind.

5. UNTERAUFTRAGSVERARBEITER

5.1. Ausschließlich zum Zweck der Bereitstellung der Gegenstand des Vertrags bildenden Dienste und im Einklang mit den Bestimmungen dieses Auftragsverarbeitungsvertrags können die Personenbezogenen Daten von durch den Auftragsverarbeiter bestimmten Unterauftragsverarbeitern verarbeitet werden.

5.2. Der Auftragsverarbeiter kann sich für die tatsächliche Erbringung eines oder mehrerer Dienste anderer Gesellschaften der Namirial-Gruppe bedienen. Die Gesellschaft der Namirial-Gruppe, die einen bestimmten Dienst tatsächlich erbringt (das „Erbringende Unternehmen"), wird für jeden Dienst im jeweiligen Verarbeitungsblatt bestimmt. Ist das Erbringende Unternehmen nicht mit dem Auftragsverarbeiter identisch, so wird es auf der Grundlage konzerninterner, mit Artikel 28 DSGVO konformer Vereinbarungen zwischen den Gesellschaften der Namirial-Gruppe tätig, die bereits vor und unabhängig von diesem Auftragsverarbeitungsvertrag bestehen. Der Verantwortliche nimmt dies mit der Unterzeichnung dieses Auftragsverarbeitungsvertrags zur Kenntnis. Ist das Erbringende Unternehmen mit dem Auftragsverarbeiter identisch, werden die im Verarbeitungsblatt aufgeführten Unterauftragsverarbeiter unmittelbar vom Auftragsverarbeiter selbst vertraglich gebunden. In jedem Fall bleibt der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Verarbeitungstätigkeiten, die das Erbringende Unternehmen und dessen Unterauftragsverarbeiter im Auftrag des Verantwortlichen nach diesem Auftragsverarbeitungsvertrag durchführen, voll verantwortlich.

5.3. Jede Verarbeitungstätigkeit, für die das Erbringende Unternehmen in einer anderen datenschutzrechtlichen Rolle handelt, wird im jeweiligen Verarbeitungsblatt bestimmt und unterliegt nicht diesem Auftragsverarbeitungsvertrag, sofern nicht ausdrücklich etwas anderes vorgesehen ist.

5.4. Der Auftragsverarbeiter verpflichtet sich, seine Unterauftragsverarbeiter unter Personen auszuwählen, deren Erfahrung, Fähigkeiten und Zuverlässigkeit hinreichende Garantien für die Umsetzung geeigneter Sicherheitsmaßnahmen bieten, sodass die Verarbeitung sämtliche Anforderungen des Anwendbaren Datenschutzrechts erfüllt und den Schutz der Rechte der Betroffenen Person gewährleistet. Zu diesem Zweck verpflichtet sich der Auftragsverarbeiter, mit den Unterauftragsverarbeitern gesonderte Verträge oder andere verbindliche Rechtsinstrumente abzuschließen, in denen der Auftragsverarbeiter deren Aufgaben im Einzelnen beschreibt und von ihnen die Einhaltung derselben Pflichten verlangt, die der Verantwortliche dem Auftragsverarbeiter nach dem Anwendbaren Datenschutzrecht und diesem Auftragsverarbeitungsvertrag auferlegt.

5.5. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, erkennt der Auftragsverarbeiter an, dass er gegenüber dem Verantwortlichen für das Verhalten dieses Unterauftragsverarbeiters voll verantwortlich bleibt. Der Auftragsverarbeiter verpflichtet sich daher, den Verantwortlichen von allen Schäden, Ansprüchen und Schadensersatzforderungen freizustellen und schadlos zu halten, die gegen den Verantwortlichen infolge der Nichterfüllung der dem Unterauftragsverarbeiter obliegenden Pflichten und, allgemeiner, infolge jeglichen Verstoßes des Unterauftragsverarbeiters sowie seiner Subunternehmer und/oder befugten Personen gegen das Anwendbare Datenschutzrecht geltend gemacht werden.

5.6. Die Verarbeitungsblätter bestimmen und führen die vom Auftragsverarbeiter bestellten und vom Verantwortlichen bereits genehmigten Unterauftragsverarbeiter auf. Der Auftragsverarbeiter verpflichtet sich ferner, den Verantwortlichen schriftlich über jede beabsichtigte Änderung oder Ersetzung von Unterauftragsverarbeitern zu informieren und dem Verantwortlichen damit die Möglichkeit zu geben, gegen diese Änderungen innerhalb von 30 (dreißig) Tagen nach Erhalt der entsprechenden Mitteilung Einspruch zu erheben.

5.7. Die Mitteilung nach dem vorstehenden Absatz kann alternativ auch durch Veröffentlichung der aktualisierten Liste der Unterauftragsverarbeiter im Bereich „Dokumentation" auf der Website des Anbieters erfolgen, die über die in Anlage A zu den Allgemeinen Bedingungen angegebenen Kontaktdaten zugänglich ist.

6. ÜBERMITTLUNG PERSONENBEZOGENER DATEN

6.1. Der Auftragsverarbeiter erklärt, die Personenbezogenen Daten nicht außerhalb des EWR zu übermitteln, sofern er hierzu nicht vorab und ausdrücklich schriftlich vom Verantwortlichen ermächtigt wurde. Im Falle einer Ermächtigung darf der Auftragsverarbeiter die Personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen und insbesondere unter vollständiger Einhaltung der Art. 44, 45, 46 und 49 DSGVO übermitteln. Die im von den Parteien unterzeichneten Verarbeitungsblatt angegebenen Übermittlungen und Unterauftragsverarbeiter außerhalb des EWR gelten als genehmigt.

6.2. Ist eine Übermittlung an ein Drittland oder eine internationale Organisation nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, erforderlich, ohne Gegenstand einer besonderen Weisung des Verantwortlichen gewesen zu sein, so gelten die in Artikel 3.7 vorgesehenen Informations-, Prüf-

und Dokumentationspflichten sowie, soweit anwendbar, die Bestimmungen von Artikel 48 und Kapitel V DSGVO.

6.3. Bei jeder Übermittlung Personenbezogener Daten außerhalb des EWR ist der Auftragsverarbeiter, soweit für das Bestimmungsland der Personenbezogenen Daten kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, verpflichtet, die Standardvertragsklauseln in ihrer jeweils zuletzt von der Europäischen Kommission angenommenen Fassung zu unterzeichnen und von den Empfängern der Personenbezogenen Daten unterzeichnen zu lassen, wobei er sicherstellt, dass die darin enthaltenen Pflichten auch gegenüber etwaigen weiteren Empfängern der Personenbezogenen Daten im Falle eines sogenannten *onward transfer* gewährleistet werden. Sofern und soweit erforderlich, hat der Auftragsverarbeiter darüber hinaus die Ergreifung etwaiger zusätzlicher Sicherheitsmaßnahmen im Einklang mit den Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten sowie mit den anwendbaren Leitlinien des Europäischen Datenschutzausschusses („EDSA“) zu vereinbaren.

7. UNTERSTÜTZUNG DES VERANTWORTLICHEN

7.1. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen dabei zu unterstützen, die Pflichten zu erfüllen, die das Anwendbare Datenschutzrecht den Verantwortlichen auferlegt, wie beispielsweise und nicht abschließend die Pflichten:

a. eine Verletzung des Schutzes Personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt wurde, der zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt;
b. eine Datenschutz-Folgenabschätzung (DSFA) in Bezug auf die durch diesen Auftragsverarbeitungsvertrag geregelte Verarbeitung durchzuführen, sofern diese Verarbeitung die Merkmale gemäß Art. 35 DSGVO aufweist;
c. die zuständige Aufsichtsbehörde gemäß Art. 36 DSGVO zu konsultieren, wenn aus einer DSFA hervorgeht, dass die durch diesen Auftragsverarbeitungsvertrag geregelte Verarbeitung ein hohes Risiko zur Folge hätte, sofern keine Maßnahmen zur Eindämmung des Risikos getroffen werden;
d. Anträge auf Ausübung der Rechte der Betroffenen Personen gemäß Kapitel III DSGVO zu beantworten. Gehen solche Anträge unmittelbar beim Auftragsverarbeiter ein, so hat der Auftragsverarbeiter (i) den Verantwortlichen unverzüglich schriftlich unter Beifügung einer Kopie des Antrags zu informieren und (ii) den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen im Rahmen seiner Zuständigkeit bei der Erfüllung dieser Anträge zu unterstützen.

8. VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

8.1. Erlangt der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes Personenbezogener Daten, die – auch mittelbar – die im Auftrag des Verantwortlichen eingesetzten Systeme und Verarbeitungsvorgänge oder die Gegenstand dieses Auftragsverarbeitungsvertrags bildenden Personenbezogenen Daten betrifft oder betreffen kann, verpflichtet sich der Auftragsverarbeiter, den Verantwortlichen durch eine förmliche Mitteilung an die Benachrichtigungs-E-Mail unverzüglich und spätestens binnen 24 (vierundzwanzig) Stunden, nachdem er Kenntnis von der Verletzung des Schutzes Personenbezogener Daten erlangt hat, zu informieren.

8.2. Nach der Feststellung einer Anomalie oder einer vermuteten Verletzung des Schutzes der Gegenstand dieses Auftragsverarbeitungsvertrags bildenden Personenbezogenen Daten ist der Auftragsverarbeiter verpflichtet, eine vorläufige Analyse einzuleiten, die darauf abzielt, die Daten zu der Anomalie und in jedem Fall alle für die Einstufung und Behandlung der Verletzung erforderlichen Informationen zu erheben, einschließlich der Einzelheiten zur Art des Vorfalls, zu den betroffenen Daten, zu den ergriffenen Maßnahmen und zum zeitlichen Ablauf der Maßnahmen.

8.3. Der Auftragsverarbeiter verpflichtet sich, die Einhaltung der vorgenannten Fristen sicherzustellen und den Verantwortlichen von etwaigen Schäden, Ansprüchen und Schadensersatzforderungen freizustellen und schadlos zu halten, die gegenüber dem Verantwortlichen infolge der Nichteinhaltung der dem Auftragsverarbeiter obliegenden Pflichten durch diesen und, allgemeiner, infolge jeglicher Verletzung des Anwendbaren Datenschutzrechts durch den Auftragsverarbeiter und seine Subunternehmer und/oder Befugten Personen geltend gemacht werden.

8.4. Im Falle einer Verletzung des Schutzes Personenbezogener Daten verpflichtet sich der Auftragsverarbeiter, im Rahmen seiner Zuständigkeit und der ihm nach dem Vertrag obliegenden Aufgaben mit dem Verantwortlichen und den zuständigen Aufsichtsbehörden umfassend zusammenzuarbeiten, um alle

anwendbaren gesetzlichen Pflichten zu erfüllen (z. B. Meldepflicht gegenüber der Aufsichtsbehörde, etwaige Benachrichtigung der Betroffenen Personen, Ergreifung geeigneter Maßnahmen zur Minderung oder Vermeidung von Risiken und Schäden). In diesem Sinne verpflichtet sich der Verantwortliche, dem Auftragsverarbeiter unverzüglich jede mit den zuständigen Aufsichtsbehörden ausgetauschte Kommunikation nachzuweisen, in die der Auftragsverarbeiter in irgendeiner Weise einbezogen ist oder in der er erwähnt wird.

9. LAUFZEIT. LÖSCHUNG UND RÜCKGABE DER PERSONENBEZOGENEN DATEN

9.1. Die Bestellung zum Auftragsverarbeiter nach diesem Auftragsverarbeitungsvertrag gilt für dieselbe Laufzeit wie der Vertrag, vorbehaltlich eines vorzeitigen Widerrufs; in diesem Fall bleibt die Bestellung so lange wirksam, wie dies für den Abschluss der zur Beendigung des Verhältnisses zwischen den Parteien oder zur Erfüllung der diesen obliegenden gesetzlichen Pflichten erforderlichen Verarbeitungsvorgänge notwendig ist.

9.2. Nach Beendigung der übertragenen Verarbeitungsvorgänge sowie bei Beendigung des Vertragsverhältnisses mit dem Auftragsverarbeiter aus welchem Grund auch immer ist Letzterer nach Wahl des Verantwortlichen verpflichtet, (i) dem Verantwortlichen die Gegenstand der Verarbeitung bildenden Personenbezogenen Daten zurückzugeben oder (ii) die Personenbezogenen Daten und sämtliche Kopien davon vollständig zu vernichten, ausgenommen die Fälle, in denen die Aufbewahrung der Daten nach dem Unionsrecht oder dem Recht eines Mitgliedstaats vorgeschrieben ist (z. B. buchhalterische oder steuerliche Pflichten) oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Die aufgrund der vorgenannten Ausnahmen aufbewahrten Daten sowie die aus technischen Gründen nicht sofort löschbaren Sicherungskopien werden in geschützter Form aufbewahrt, keiner weiteren Verarbeitung unterzogen und nach Ablauf der jeweiligen Aufbewahrungsfrist oder gemäß den üblichen Überschreibungszyklen gelöscht. In beiden Fällen hat der Auftragsverarbeiter dem Verantwortlichen eine schriftliche Erklärung über die erfolgte Rückgabe oder Löschung unter Angabe etwaiger der vorgenannten Ausnahmen vorzulegen.

10. AUDITS UND INSPEKTIONEN

10.1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Auftragsverarbeitungsvertrag und dem Anwendbaren Datenschutzrecht zur Verfügung und ermöglicht Audits, einschließlich Inspektionen, die vom Verantwortlichen und/oder einem von diesem benannten Dritten durchgeführt werden, und trägt zu diesen bei.

10.2. Die Audits werden vorzugsweise in Form einer Dokumentenprüfung oder mittels Interviews durchgeführt, auch anhand von Fragebögen, Auskunftsersuchen, der Prüfung von Zertifizierungen, Auditberichten, Richtlinien, Verfahren und sonstigen vom Auftragsverarbeiter zur Verfügung gestellten Compliance-Unterlagen.

10.3. Außer im Falle einer Verletzung des Schutzes Personenbezogener Daten mit erheblichen Auswirkungen auf die im Auftrag des Verantwortlichen verarbeiteten Personenbezogenen Daten oder im Falle, dass eine zuständige Aufsichtsbehörde gegenüber dem Auftragsverarbeiter eine Sanktion oder eine verbindliche Maßnahme mit unmittelbarem Bezug zu den Diensten erlassen hat, hat der Verantwortliche:

(a) dem Auftragsverarbeiter eine schriftliche Vorankündigung von mindestens dreißig (30) Tagen zukommen zu lassen;

(b) nicht mehr als ein Audit pro Kalenderjahr durchzuführen;

(c) sicherzustellen, dass das Audit zwei (2) volle Arbeitstage nicht überschreitet; und

(d) das Audit so durchzuführen, dass die gewöhnlichen betrieblichen Tätigkeiten des Auftragsverarbeiters nicht unangemessen beeinträchtigt werden.

10.4. Der Verantwortliche trägt sämtliche Kosten, Auslagen und Vergütungen im Zusammenhang mit dem Audit, einschließlich etwaiger Kosten der vom Verantwortlichen beauftragten Auditoren. Erfordert das Audit Zeit oder Ressourcen über die in Artikel 10.3 genannten Grenzen hinaus, so informiert der Auftragsverarbeiter den Verantwortlichen vorab darüber, und die Parteien vereinbaren nach Treu und Glauben, den Umfang des Audits zu reduzieren oder die zusätzlichen Kosten dem Verantwortlichen aufzuerlegen.

10.5. Wird das Audit mittels Fragebögen, Formularen oder Dokumentenanforderungen durchgeführt, so wird dem Auftragsverarbeiter eine angemessene Frist zur Beantwortung eingeräumt, die nicht weniger als dreißig (30) Tage ab Eingang der vollständigen Anfrage betragen darf. Diese Frist kann verlängert werden, soweit dies

unter Berücksichtigung der Komplexität der Anfrage und der Verfügbarkeit des Personals des Auftragsverarbeiters vernünftigerweise erforderlich ist.

10.6. Der Verantwortliche und jeder von ihm beauftragte Dritte verwenden die im Rahmen des Audits erlangten Informationen ausschließlich zum Zweck der Überprüfung der Einhaltung dieses Auftragsverarbeitungsvertrags und behandeln diese Informationen streng vertraulich.

11. MITTEILUNGEN ZWISCHEN DEN PARTEIEN

11.1. Für die Zwecke dieses Auftragsverarbeitungsvertrags erklärt der Auftragsverarbeiter, einen Datenschutzbeauftragten bestellt und/oder, soweit anwendbar, einen entsprechenden Datenschutzansprechpartner im Einklang mit dem Anwendbaren Datenschutzrecht benannt zu haben. Die entsprechenden Kontaktdaten des Auftragsverarbeiters, einschließlich der Kontaktdaten des DSB oder des Datenschutzansprechpartners, sind die für den jeweiligen Anbieter in Anlage A zu den Allgemeinen Bedingungen angegebenen, wie im Kommerziellen Angebot bestimmt. Diese Kontaktdaten sind für sämtliche Mitteilungen in Angelegenheiten des Datenschutzes nach diesem Auftragsverarbeitungsvertrag zu verwenden.

11.2. Der Auftragsverarbeiter kontaktiert den Verantwortlichen in allen in diesem Auftragsverarbeitungsvertrag vorgesehenen Fällen durch eine an die vom Verantwortlichen mitgeteilte Benachrichtigungs-E-Mail übermittelte Mitteilung.

11.3. Die Parteien verpflichten sich, einander jede Änderung ihrer jeweiligen Kontaktadressen unverzüglich mitzuteilen. Unterbleibt eine solche rechtzeitige Mitteilung, gelten die an die nicht aktualisierte Adresse gesandten Mitteilungen als gültig und wirksam.

ANLAGE I

DEFINITIONEN

a) „**Auftragsverarbeitungsvertrag“** bezeichnet diesen Allgemeinen Auftragsverarbeitungsvertrag einschließlich der Vorbemerkungen und der Anlagen;

b) „**Systemadministratoren“** bezeichnet die Befugten Personen, die für die Verwaltung und Wartung eines Verarbeitungssystems oder seiner Komponenten zuständig sind, wie sie gemäß Artikel 32 DSGVO und den anwendbaren nationalen Bestimmungen über die Zuweisung der Funktionen eines Systemadministrators bestimmt werden und, soweit einschlägig, im jeweiligen Verarbeitungsblatt näher festgelegt sind;

c) „**Aufsichtsbehörde“** bezeichnet jede unabhängige Aufsichtsbehörde im Sinne von Kapitel VI DSGVO, die für die Überwachung und Durchsetzung der gesetzlichen Bestimmungen zum Schutz Personenbezogener Daten in Bezug auf die in Ausführung des Vertrags durchgeführte Verarbeitung Personenbezogener Daten zuständig ist;

d) **„Besondere Kategorien Personenbezogener Daten“** bezeichnet Personenbezogene Daten, aus denen die rassische oder 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, wie in Art. 9 DSGVO bestimmt;

e) „**Standardvertragsklauseln“** bezeichnet die von der Europäischen Kommission mit Beschluss (EU) 2021/914 vom 4. Juni 2021 angenommenen Klauseln für die Übermittlung Personenbezogener Daten von einem in der Europäischen Union („EU“) / im Europäischen Wirtschaftsraum („EWR“) niedergelassenen Verantwortlichen an eine Stelle außerhalb der EU bzw. des EWR, die als Auftragsverarbeiter handelt;

f) „**Vertrag“** bezeichnet den zwischen den Parteien unterzeichneten Vertrag über die Bereitstellung der Dienste;

g) „**Personenbezogene Daten“** bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Betroffene Person) beziehen und vom Auftragsverarbeiter im Auftrag des Verantwortlichen im Zusammenhang mit der Ausführung des Vertrags verarbeitet werden;

h) „**Rechte der Betroffenen Person“** bezeichnet die der Betroffenen Person durch das Anwendbare Datenschutzrecht zuerkannten Rechte. Soweit die DSGVO anwendbar ist, sind unter „Rechten der Betroffenen Person“ beispielsweise das Recht, vom Verantwortlichen Auskunft über die Personenbezogenen Daten sowie deren Berichtigung oder Löschung zu verlangen, das Recht auf Einschränkung der Verarbeitung der Daten der Betroffenen Person oder das Recht auf Widerspruch gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit zu verstehen;

i) „**Benachrichtigungs-E-Mail“** bezeichnet die E-Mail-Adresse(n), die der Kunde bei Unterzeichnung des Vertrags angegeben oder dem Auftragsverarbeiter über einen anderen offiziellen Kanal mitgeteilt hat und unter der/denen der Kunde die Benachrichtigungen des Auftragsverarbeiters zu erhalten wünscht;

j) „**Anwendbares Datenschutzrecht“** bezeichnet alle Gesetze und Verordnungen zum Schutz Personenbezogener Daten, die auf die dem Vertrag zugrunde liegende Verarbeitung Personenbezogener Daten anwendbar sind, einschließlich der Verordnung (EU) 2016/679 („DSGVO“), etwaiger anwendbarer nationaler Datenschutzgesetze und -verordnungen der EU-Mitgliedstaaten, soweit diese nach ihrem räumlichen und sachlichen Anwendungsbereich anwendbar sind, sowie aller von der zuständigen Aufsichtsbehörde erlassenen verbindlichen Maßnahmen, Beschlüsse, Leitlinien oder Vorgaben;

k) „**Sicherheitsmaßnahmen“** bezeichnet die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, die geeignet sind, ein angemessenes Sicherheitsniveau der Personenbezogenen Daten zu gewährleisten, sowie alle Maßnahmen, die erforderlich sind, um jedes vernünftigerweise vorhersehbare Risiko der unbeabsichtigten oder unrechtmäßigen Vernichtung, des Verlusts, der Veränderung, der unbefugten Offenlegung der verarbeiteten Personenbezogenen Daten oder des unbefugten Zugangs zu ihnen zu verhindern oder zumindest auf ein Mindestmaß zu reduzieren;

l) „**Befugte Personen“** bezeichnet die natürlichen Personen innerhalb der Organisationsstruktur des Auftragsverarbeiters, die ausdrücklich schriftlich bestimmt und befugt sind, im Rahmen der Ausführung des Vertrags auf die Personenbezogenen Daten zuzugreifen und diese zu verarbeiten, und die unter der Aufsicht und nach den Weisungen des Auftragsverarbeiters handeln;

m) „**Auftragsverarbeiter“** bezeichnet allgemein eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet;

n) „**Dienste“** bezeichnet die nach dem Vertrag erbrachten Dienste;

o) „**Systeme des Verantwortlichen“** bezeichnet die gegebenenfalls vom Verantwortlichen und/oder von durch diesen beauftragten Dritten zur Verfügung gestellten Infrastrukturen und Systeme, auf denen der Auftragsverarbeiter die Verarbeitung durchzuführen hat;

p) „**Unterauftragsverarbeiter“** bezeichnet eine vom Auftragsverarbeiter bestimmte Stelle, die die dem Auftragsverarbeiter übertragene Verarbeitung Personenbezogener Daten ganz oder teilweise unter Einhaltung der vom Verantwortlichen festgelegten Pflichten und Weisungen durchführt und von diesem ausdrücklich genehmigt wurde;

q) „**Konzerninterner Unterauftragsverarbeiter“** bezeichnet die zur Namirial-Gruppe gehörende Gesellschaft, die auf der Grundlage bereits bestehender, mit Artikel 28 DSGVO konformer und von diesem Auftragsverarbeitungsvertrag getrennter konzerninterner Vereinbarungen zwischen den Gesellschaften der Namirial-Gruppe als Unterauftragsverarbeiter für die materielle Erbringung eines oder mehrerer Dienste tätig wird;

r) „**Erbringendes Unternehmen“** bezeichnet die Gesellschaft der Namirial-Gruppe, die den jeweiligen Gegenstand des einzelnen Verarbeitungsblatts bildenden Dienst materiell erbringt. Das Erbringende Unternehmen kann mit dem Auftragsverarbeiter identisch sein oder als dessen Konzerninterner Unterauftragsverarbeiter tätig werden. In beiden Fällen wird es im jeweiligen Verarbeitungsblatt bestimmt;

s) „**Verantwortlicher“** bezeichnet allgemein die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung Personenbezogener Daten entscheidet;

t) „**Verarbeitung“** bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten oder Sätzen Personenbezogener 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.

ANLAGE II

TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMASSNAHMEN

1. ORGANISATORISCHE SICHERHEITSMASSNAHMEN

ART DER MASSNAHME	BESCHREIBUNG
Interne Richtlinien und Regelungen	Der Auftragsverarbeiter hat eine Reihe interner Richtlinien, Verfahren und Regelungen eingeführt, die für sämtliches zur Verarbeitung Personenbezogener Daten befugtes Personal verbindlich sind. Diese Richtlinien und Leitlinien legen die Regeln für die sichere Nutzung der IT-Ressourcen fest und sehen spezifische interne Vorschriften für den Umgang mit Informationen vor, deren Einhaltung für alle Nutzer verpflichtend ist. Ziel ist es, die Einhaltung der Grundsätze der Vertraulichkeit, Integrität und Verfügbarkeit der Personenbezogenen Daten zu gewährleisten und die Risiken eines unbefugten Zugriffs oder einer missbräuchlichen Nutzung von Informationen in allen Gesellschaften der Gruppe zu minimieren.
Zugriffsberechtigung und logische Kontrollen	Der Auftragsverarbeiter legt die Zugriffsprofile nach dem Prinzip der geringsten für die Ausführung der zugewiesenen Aufgaben erforderlichen Berechtigung fest. Die Berechtigungsprofile werden vor Beginn der Verarbeitung bestimmt und konfiguriert, sodass der Zugriff auf die für die Durchführung der Verarbeitungsvorgänge erforderlichen Personenbezogenen Daten beschränkt ist. Für besonders sensible Vorgänge wird eine Zwei-Faktor-Authentifizierung (MFA) eingesetzt, um die Zugriffssicherheit zu erhöhen. Diese Profile werden regelmäßig daraufhin überprüft, ob die Voraussetzungen für die Beibehaltung der zugewiesenen Profile weiterhin vorliegen.
Zugriffsüberwachung	Die Protokollierung und Überwachung der Zugriffe auf Systeme, die Personenbezogene Daten verarbeiten, wird gewährleistet, einschließlich einer regelmäßigen Auswertung der Logs zur Erkennung etwaiger Anomalien oder verdächtiger Aktivitäten.
Change Management	Der Auftragsverarbeiter hat ein spezifisches Verfahren eingeführt, mit dem er den Change-Management-Prozess im Hinblick auf die Einführung etwaiger technologischer Neuerungen oder Änderungen seiner Organisationsstruktur regelt.
Incident Management und Business Continuity	Der Auftragsverarbeiter hat ein spezifisches Incident-Management-Verfahren eingerichtet, um die Wiederherstellung des normalen Dienstbetriebs in kürzestmöglicher Zeit unter Aufrechterhaltung des bestmöglichen Serviceniveaus zu gewährleisten. Vorfälle werden nach Schweregrad und Auswirkungen auf die Personenbezogenen Daten eingestuft. Das Personal ist darin geschult, Sicherheitsereignisse zu bewältigen und die Eindämmungsverfahren durchzuführen. Es sind regelmäßige Tests der Reaktionsfähigkeit der Organisation auf Vorfälle vorgesehen. Ein Business Continuity Plan ist implementiert, um die Resilienz der Dienste auch in Notfällen zu gewährleisten.
Maßnahmen zur Gewährleistung der Speicherbegrenzung	Der Auftragsverarbeiter folgt den Grundsätzen Data Protection by Design und by Default. Technische Maßnahmen: Es werden nicht mehr Personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind; Verwendung datenschutzfreundlicher

	Voreinstellungen. Organisatorische Maßnahmen: Datenschutzrichtlinie nach den Grundsätzen „privacy by design / by default“, enthalten in der SCS-P14 Group Privacy and Personal Data Protection Policy; Durchführung der Sicherheitskontrollen nach OWASP Secure Mobile Development (siehe SCS-P08 Group Secure Coding Policy); Analyse des Perimeters der Webanwendungen.
Data Breach	Der Auftragsverarbeiter hat ein eigenes Verfahren zur Behandlung von Ereignissen und Vorfällen mit potenziellen Auswirkungen auf die Personenbezogenen Daten eingeführt, das Rollen und Verantwortlichkeiten, den Erkennungsprozess (vermutet oder festgestellt), die Ergreifung von Gegenmaßnahmen, die Reaktion auf den Vorfall bzw. die Verletzung und deren Eindämmung sowie die Modalitäten festlegt, nach denen Verletzungen des Schutzes Personenbezogener Daten dem Verantwortlichen unverzüglich mitzuteilen sind. Soweit es den Auftragsverarbeiter betrifft, bestimmt dieses Verfahren mindestens: die Art der Verletzung des Schutzes Personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen Datensätze; die wahrscheinlichen Folgen der Verletzung des Schutzes Personenbezogener Daten; die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes Personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
Schulung	Um ein angemessenes Sensibilisierungsniveau zu gewährleisten, führt der Auftragsverarbeiter regelmäßige Schulungen zur ordnungsgemäßen Verarbeitung Personenbezogener Daten und zur Informationssicherheit durch. Die Schulung ist für sämtliches Personal, das auf Personenbezogene Daten zugreift, verpflichtend. Es sind Tests und Überprüfungen vorgesehen, um den Kenntnisstand hinsichtlich der Sicherheitsrichtlinien zu bewerten. Es werden Kampagnen zur Simulation von Cyberangriffen (z. B. Phishing-Tests) durchgeführt, um das Personal für die häufigsten Bedrohungen zu sensibilisieren. Die Schulung wird regelmäßig aktualisiert, um regulatorische und technologische Entwicklungen widerzuspiegeln.
Management der Unterauftragsverarbeiter	Setzt der Auftragsverarbeiter Unterauftragsverarbeiter ein, werden strenge Kontrollen durchgeführt, um deren Einhaltung der geforderten Sicherheitsmaßnahmen zu überprüfen. Jeder Unterauftragsverarbeiter ist verpflichtet, Sicherheitsstandards einzuhalten, die denen des Auftragsverarbeiters gleichwertig sind. Es sind regelmäßige Audits und Inspektionen zur Überprüfung der Compliance der Lieferanten vorgesehen. Der Auftragsverarbeiter führt ein aktuelles Verzeichnis der Unterauftragsverarbeiter.
Datensicherung und -wiederherstellung	Zur Gewährleistung der Datenverfügbarkeit und der Ausfallsicherheit implementiert der Auftragsverarbeiter ein Backup- und Disaster-Recovery-System, das Folgendes vorsieht: regelmäßige Backups mit festgelegten Aufbewahrungsrichtlinien; Schutz der Backups durch Verschlüsselung und kontrollierten Zugriff; regelmäßige Tests, um die schnelle Wiederherstellung der Daten im Bedarfsfall zu gewährleisten; Replikation der Daten in sicheren Rechenzentren, um den Verlust kritischer Informationen zu verhindern.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und	Die internen Richtlinien zu den Sicherheitsmaßnahmen werden im Rahmen der laufenden internen Audits sowie jährlich durch unabhängige, externe und akkreditierte Zertifizierungsstellen im Rahmen der Überwachungs- und Rezertifizierungsaudits nach ISO 9001

organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	und ISO 27001 regelmäßig überprüft und hinsichtlich ihrer Angemessenheit und Wirksamkeit bestätigt.
Benennung des CISO	Um ein angemessenes Niveau der Informationssicherheit und die Einhaltung der anwendbaren Vorschriften zu gewährleisten, hat der Auftragsverarbeiter einen Chief Information Security Officer (CISO) benannt, dessen Hauptaufgaben darin bestehen: die Umsetzung und Wirksamkeit der zum Schutz der Personenbezogenen Daten ergriffenen Sicherheitsmaßnahmen zu überwachen; die Entwicklung der Cyberbedrohungen zu beobachten und die kontinuierliche Aktualisierung der Sicherheitsrichtlinien zu fördern; die Maßnahmen zur Reaktion auf Sicherheitsvorfälle zu koordinieren; Strategien zur Verbesserung der Sicherheit zum Schutz der Unternehmenswerte festzulegen. Der CISO arbeitet eng mit den übrigen an der Steuerung der Sicherheit und des Datenschutzes beteiligten Unternehmensfunktionen zusammen.
Konformitätszertifizierungen	Die vollständige Liste der Zertifizierungen des Anbieters ist unter folgender Adresse abrufbar: https://www.namirial.com/it/company/certificazioni/

2. TECHNISCHE SICHERHEITSMASSNAHMEN

ART DER MASSNAHME	BESCHREIBUNG
Capacity Planning und Leistungsüberwachung	Der Auftragsverarbeiter führt einen kontinuierlichen Prozess der Analyse und Optimierung der IT-Ressourcen durch, um eine für die Bereitstellung der Dienste und die Verwaltung der Personenbezogenen Daten angemessene Leistung zu gewährleisten. Das System sieht eine proaktive Überwachung der Rechen-, Speicher- und Netzwerkbandbreitenkapazität vor. Es wird eine Prognose des künftigen Bedarfs erstellt, um Skalierbarkeit und Betriebskontinuität zu gewährleisten. Es sind regelmäßige Last- und Resilienztests vorgesehen, um kritischen Situationen aufgrund von Überlastungen oder Nutzungsspitzen vorzubeugen.
Systemsicherheit und -härtung	Um Schwachstellen zu minimieren und den Schutz der IT-Infrastrukturen zu verbessern, wendet der Auftragsverarbeiter Härtungsmaßnahmen (Hardening) auf Betriebssysteme, Anwendungssoftware und Unternehmensnetzwerke an. Die Systeme werden nach Sicherheits-Best-Practices konfiguriert, um die Risikoexposition zu begrenzen. Nicht erforderliche Funktionen werden deaktiviert und Zugriffsbeschränkungen auf Netzwerkdienste angewendet. Die Konfigurationen werden regelmäßig überprüft und entsprechend der Entwicklung der Bedrohungslage aktualisiert.
Patch Management und Sicherheitsupdates	Der Auftragsverarbeiter unterhält einen strukturierten Prozess für das Update-Management, um den Schutz vor Software-Schwachstellen zu gewährleisten. Sicherheitsupdates werden je nach Schweregrad der Schwachstellen zeitnah eingespielt. Es sind Testverfahren vor der Freigabe vorgesehen, um negative Auswirkungen auf die Dienstkontinuität zu vermeiden. Kritische Systeme werden regelmäßig

	überprüft, um etwaige noch nicht behobene Schwachstellen zu erkennen.
Schutz von Netzwerk und Systemen	Die Personenbezogenen Daten sind durch fortschrittliche Lösungen für Perimetersicherheit und Intrusion Detection geschützt, darunter: Firewalls der nächsten Generation zur erweiterten Filterung des Datenverkehrs; IDPS-Systeme (Intrusion Detection & Prevention System) zur Erkennung und Blockierung verdächtiger Aktivitäten; Netzwerksegmentierung zur Begrenzung der Ausbreitungsrisiken im Falle eines Angriffs.
Schutz vor Malware und Cyberbedrohungen	Der Auftragsverarbeiter setzt fortschrittliche Schutzwerkzeuge ein, um die Risiken durch Malware und Cyberangriffe zu mindern: regelmäßig aktualisierte Antiviren- und Anti-Malware-Programme zur Erkennung und Blockierung von Bedrohungen in Echtzeit; Sandboxing-Systeme zur Analyse und Isolierung verdächtiger Dateien vor deren Ausführung; Bedrohungsüberwachung zur Abwehr von Zero-Day-Angriffen.
Sicherheit der Kommunikation und Schutz der Datenübertragung	Der Auftragsverarbeiter setzt fortschrittliche Sicherheitsprotokolle ein, um die Integrität und Vertraulichkeit der Kommunikation zu gewährleisten: Ende-zu-Ende-Verschlüsselung zum Schutz der Daten bei der Übertragung; Authentifizierung und digitale Zertifikate zur Überprüfung der Integrität der Kommunikation; VPN-Segmentierung und private Netzwerke zur Verringerung des Risikos des Abfangens.
Physischer Schutz der IT-Infrastrukturen	Der Zugang zu den Räumlichkeiten, in denen Personenbezogene Daten gespeichert oder verarbeitet werden, unterliegt verstärkten physischen Sicherheitsmaßnahmen: kontrollierter Zugang mit Badge-Systemen, Zutrittsprotokollierung und vorheriger Genehmigung. Videoüberwachung und Einbruchmeldeanlagen sind rund um die Uhr (24/7) aktiv. Umgebungsbezogene Sicherheitsmaßnahmen, darunter Brandschutzsysteme, Redundanz der Elektro- und Klimaanlagen, USV und Notstromaggregate zur Gewährleistung der Betriebskontinuität. Notfall- und Disaster-Recovery-Verfahren mit regelmäßigen Simulationen zur Erprobung der Pläne zur Reaktion auf Vorfälle.
Verwaltung der Zugangsdaten und Zugang zu den Systemen	Zur Verhinderung unbefugter Zugriffe implementiert der Auftragsverarbeiter ein strenges System zur Authentifizierung und Verwaltung der Zugangsdaten: Multi-Faktor-Authentifizierung für Nutzer mit Zugriff auf Personenbezogene Daten und sensible Informationen; erweiterte Passwortrichtlinie mit Anforderungen an Länge, Komplexität und regelmäßigen Ablauf; sofortiger Entzug der Zugriffsrechte bei Beendigung des Arbeitsverhältnisses oder Änderung der Aufgaben.
Verwaltung der Systemadministratoren	Die Systemadministratoren unterliegen als Personen mit erweiterten Berechtigungen einer strengen Kontroll- und Überwachungsregelung. Der Auftragsverarbeiter führt ein aktuelles und dokumentiertes Verzeichnis der Systemadministratoren. Die administrativen Tätigkeiten werden nachverfolgt und in geschützten und unveränderbaren Logs aufgezeichnet. Es werden regelmäßige Audits durchgeführt, um die Tätigkeit der Administratoren und die ordnungsgemäße Anwendung der Sicherheitsrichtlinien zu überprüfen.