Auftragsverarbeitungsvereinbarung (AVV)

Die Bestimmungen dieser Auftragsverarbeitungsvereinbarung (die "**Vereinbarung**") sind Bestandteil des Hauptvertrages (der "**Hauptvertrag**"), der aus den Allgemeinen Geschäftsbedingungen von Validato AG (einschliesslich aller Unternehmen, die von Zeit zu Zeit Tochtergesellschaften von Validato AG sind; im Folgenden zusammenfassend als "**Validato**" bezeichnet), wie jeweils auf der Webseite veröffentlicht, und etwaigen besonderen Vereinbarungen zwischen den Parteien.

Der Hauptvertrag wird zwischen dem Kunden (dem "**Verantwortlichen**") und Validato (dem "**Auftragsverarbeiter**"; zusammen die "**Parteien**") geschlossen und gilt, wenn der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen gemäss dem Schweizer Datenschutzgesetz, der EU-Datenschutz-Grundverordnung, der Datenschutz-Grundverordnung des Vereinigten Königreichs oder anderen gleichwertigen Bestimmungen der geltenden Datenschutzgesetze verarbeitet, sofern die Parteien keine spezifische Datenverarbeitungsvereinbarung getroffen haben.

1. Zweck

Diese Vereinbarung legt die Anforderungen fest, die der Auftragsverarbeiter bei der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen zu erfüllen hat.

Im Rahmen ihres Vertragsverhältnisses verpflichten sich beide Parteien, die geltenden Datenschutzbestimmungen jederzeit einzuhalten.

Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Anweisung des Verantwortlichen, es sei denn, dass dies aufgrund geltender Rechtsvorschriften erforderlich ist. In einem solchen Fall informiert der Auftragsverarbeiter (soweit gesetzlich zulässig) den Verantwortlichen vor der Verarbeitung über diese gesetzliche Anforderung.

2. Definitionen

In dieser Vereinbarung haben die folgenden Begriffe folgende Bedeutungen:

"**Anwendbare Datenschutzbestimmungen**" bezeichnet (sofern zutreffend) die EU-Datenschutz-Grundverordnung 2016/679 ("**DSGVO**"), das Schweizer Bundesgesetz über den Datenschutz ("**DSG**") und die Datenschutz-Grundverordnung des Vereinigten Königreichs ("**UK-DSGVO**") sowie alle anderen Datenschutzgesetze, auf die im Hauptvertrag ausdrücklich Bezug genommen wird;

"**Datensubjekt**" bezeichnet die Person, deren personenbezogene Daten gemäss dieser Vereinbarung verarbeitet werden;

"**Anweisungen**" bezeichnet die dokumentierten Anweisungen des Verantwortlichen (einschliesslich per E-Mail und im Tool des Auftragsverarbeiters) an den Auftragsverarbeiter bezüglich der Verarbeitung personenbezogener Daten;

"**Personenbezogene Daten**" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen und gemäss dieser Vereinbarung verarbeitet werden; und

"**Unterauftragsverarbeiter**" sind alle Dritten, die vom Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen beauftragt werden.

3. Beschreibung der Verarbeitungstätigkeiten

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschliesslich im Auftrag und gemäss den Anweisungen des Verantwortlichen zum Zweck der Erbringung der im Hauptvertrag festgelegten Dienstleistungen (die "**Dienstleistungen**"). Die Dienstleistungen umfassen die Überprüfung/Hintergrundüberprüfung eines Datensubjekts gemäss den Anweisungen des Verantwortlichen.

Zur Vermeidung von Unklarheiten regelt diese Vereinbarung die gesamte Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Zusammenhang mit den Dienstleistungen, einschliesslich aller Erhebungs-, Überprüfungs-, Analyse- und Berichterstattungsaktivitäten, die im Rahmen von Überprüfungen/Hintergrundüberprüfungen durchgeführt werden.

Der Auftragsverarbeiter bestimmt weder den Verwendungszweck noch die Prüfpunkte in Bezug auf welche die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung erfolgt. Der Verantwortliche bleibt der alleinige Verantwortliche für diese personenbezogenen Daten.

Die Arten von personenbezogenen Daten, die gemäss dieser Vereinbarung verarbeitet werden können, sind in Anhang A aufgeführt.

Zu den betroffenen Personen gehören (i) Mitarbeiter, Vertreter und autorisierte Nutzer des Verantwortlichen, deren personenbezogene Daten für die Tooladministration und den Support verarbeitet werden, sowie (ii) die Personen, auf die sich die Überprüfung/Hintergrundüberprüfung bezieht (z. B. Bewerber, Auftragnehmer, Kunden oder andere Personen, deren personenbezogene Daten im Zusammenhang mit der Erbringung der Dienste verarbeitet werden).

4. Laufzeit

Diese Vereinbarung tritt am Tag des Inkrafttretens des Hauptvertrages in Kraft und bleibt auch nach Beendigung (aus welchem Grund auch immer) oder Ablauf der Hauptvertrages bestehen.

5. Verpflichtungen des Auftragsverarbeiters (einschliesslich Schadloshaltung des Verantwortlichen)

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen:

- die personenbezogenen Daten ausschliesslich für die in Ziffer 1 und Ziffer 3 dieser Vereinbarung definierten Zwecke zu verarbeiten;
- die personenbezogenen Daten ausschliesslich gemäss den dokumentierten Anweisungen des Verantwortlichen (einschliesslich per E-Mail und im Tool des Auftragsverarbeiters) zu verarbeiten;
- die Vertraulichkeit der personenbezogenen Daten zu gewährleisten, vorbehaltlich der Anweisungen sowie der Offenlegung personenbezogener Daten gegenüber Dritten (z. B. ehemaligen Arbeitgebern, Behörden usw.) zur Erbringung der Dienstleistungen;
- sicherzustellen, dass jede vom Auftragsverarbeiter zur Verarbeitung personenbezogener Daten befugte Person, einschliesslich Mitarbeiter, Auftragnehmer und sonstiger Personen, die unter der Autorität des Auftragsverarbeiters handeln, angemessenen Vertraulichkeitsverpflichtungen unterliegt und eine ihrer Rolle sowie ihren Zugriffsrechten entsprechende Schulung erhält;
- den Verantwortlichen unverzüglich zu informieren, falls der Auftragsverarbeiter die Bestimmungen dieser Vereinbarung oder die geltenden Datenschutzvorschriften nicht mehr einhalten kann; und
- dem Verantwortlichen auf Anfrage Folgendes zur Verfügung zu stellen:

- schriftliche Nachweise über die kontinuierliche Einhaltung dieser Vereinbarung und der geltenden Datenschutzbestimmungen durch den Auftragsverarbeiter; und
- alle anderen Dokumente, die der Verantwortliche vernünftigerweise verlangt, um die Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter nachzuweisen (z. B. Kopien der entsprechenden Audits, ISO-Berichte (Internationale Organisation für Normung) oder ähnlicher Berichte und/oder schriftliche Bestätigungen des Auftragsverarbeiters).

Vorbehaltlich der im Hauptvertrag festgelegten Haftungsbeschränkung stellt der Auftragsverarbeiter den Verantwortlichen von allen Ansprüchen, Verlusten, Kosten (einschliesslich angemessener Anwaltskosten), Geldstrafen und sonstigen finanziellen Nachteilen frei, die dem Verantwortlichen aufgrund eines Verstosses des Auftragsverarbeiters gegen diese Vereinbarung oder die geltenden Datenschutzbestimmungen entstehen. Die Freistellungsverpflichtung des Auftragsverarbeiters gemäss dieser Vereinbarung gilt nur für Schäden, die auf einen nachweislich vorsätzlichen oder grob fahrlässigen Verstoss des Auftragsverarbeiters gegen diese Vereinbarung zurückzuführen sind. Der Auftragsverarbeiter stellt den Verantwortlichen nicht frei für (i) Verarbeitungsaktivitäten, die im Rahmen der unabhängigen Rolle des Auftragsverarbeiters als Verantwortlicher durchgeführt werden, (ii) Schäden, die durch unrichtige, unvollständige oder unrechtmässige Daten verursacht werden, die vom Verantwortlichen, seinen Nutzern oder einem Datensubjekt bereitgestellt wurden, oder (iii) Schäden, die sich aus den Anweisungen des Verantwortlichen oder der Nichteinhaltung geltender Datenschutzgesetze ergeben.

Soweit nach geltendem Recht zulässig, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen nicht für Schäden, Verluste, Ansprüche, Kosten oder regulatorische Folgen, die aus einer Verletzung der Pflichten des Verantwortlichen in seiner Eigenschaft als Verantwortlicher entstehen, einschliesslich solcher Schäden, die aus dem Fehlen einer gültigen Rechtsgrundlage, unzureichender Transparenz gegenüber den betroffenen Personen, unrichtigen oder rechtswidrigen personenbezogenen Daten, die vom oder im Auftrag des Verantwortlichen bereitgestellt wurden, oder aus rechtswidrigen Weisungen des Verantwortlichen resultieren. Nichts in diesem Nachtrag beschränkt eine Haftung, die nach den geltenden Datenschutzvorschriften nicht beschränkt werden kann, oder beeinträchtigt die gesetzlichen Rechte der betroffenen Personen.

6. Verpflichtungen des Verantwortlichen

Der Verantwortliche verpflichtet sich gegenüber dem Auftragsverarbeiter:

- sicherzustellen, dass für sämtliche personenbezogenen Daten, die dem Auftragsverarbeiter im Rahmen der Dienstleistungen übermittelt oder zugänglich gemacht werden, eine gültige Rechtsgrundlage besteht;
- sicherzustellen, dass jede Verarbeitung besonderer Kategorien personenbezogener Daten, von Daten über Straftaten oder strafrechtliche Verurteilungen, Background-Check-Daten oder sonstiger sensibler Informationen rechtmässig, erforderlich, verhältnismässig und nach den geltenden Datenschutzvorschriften sowie etwaigen anwendbaren arbeitsrechtlichen, regulatorischen oder sektorspezifischen Vorschriften zulässig ist;
- den betroffenen Personen sämtliche erforderlichen Datenschutzhinweise und Transparenzinformationen bereitzustellen, bevor der Auftragsverarbeiter mit der Erbringung der Dienstleistungen beauftragt wird, sofern keine Ausnahme nach geltendem Recht greift;
- dem Auftragsverarbeiter klare, rechtmässige und dokumentierte Weisungen zu erteilen und sicherzustellen, dass diese Weisungen jederzeit mit den geltenden Datenschutzvorschriften im Einklang stehen;

- sicherzustellen, dass die dem Auftragsverarbeiter bereitgestellten personenbezogenen Daten richtig, relevant, auf das notwendige Mass beschränkt und rechtmässig erhoben wurden;
- den Auftragsverarbeiter unverzüglich über jede Änderung von Gesetzen, Weisungen, des Leistungsumfangs, von Aufbewahrungspflichten oder Anfragen betroffener Personen zu informieren, die sich auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter auswirken können;
- sicherzustellen, dass seine autorisierten Nutzer die Plattform und Dienstleistungen des Auftragsverarbeiters im Einklang mit den geltenden Datenschutzvorschriften nutzen; und
- sämtliche erforderlichen Exporte, Downloads oder Sicherungen von Kundendaten vor Ablauf oder Beendigung der Dienstleistungen vorzunehmen, sofern nicht schriftlich etwas anderes vereinbart wurde.

7. Unterauftragsverarbeiter

Der Verantwortliche stimmt zu, dass der Auftragsverarbeiter Unterauftragsverarbeiter zur Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Verantwortlichen einsetzen darf. Der Auftragsverarbeiter führt eine öffentlich zugängliche und stets aktuelle Liste der Unterauftragsverarbeiter unter validato.com/sub-processors (die „**Liste der Unterauftragsverarbeiter**"), einschliesslich sämtlicher hundertprozentiger Tochtergesellschaften des Auftragsverarbeiters innerhalb des EWR oder der Schweiz. Sollte die Liste der Unterauftragsverarbeiter vorübergehend online nicht verfügbar sein, wird die aktuelle Liste auf Anfrage bereitgestellt.

Vor der Beauftragung eines neuen Unterauftragsverarbeiters, der noch nicht in der Liste der Unterauftragsverarbeiter aufgeführt ist, informiert der Auftragsverarbeiter den Verantwortlichen mindestens 30 Tage im Voraus schriftlich per E-Mail. Der Verantwortliche ist berechtigt, innerhalb dieses Zeitraums der Beauftragung eines solchen Unterauftragsverarbeiters zu widersprechen. Es dürfen keine personenbezogenen Daten an diesen Unterauftragsverarbeiter übermittelt werden, bevor die Mitteilungsfrist ohne Widerspruch abgelaufen ist oder ein erhobener Widerspruch geklärt wurde.

Im Zusammenhang mit den Dienstleistungen des Auftragsverarbeiters im Bereich Screening und Background Checks führt der Auftragsverarbeiter eine gesonderte Liste von Unterauftragsverarbeitern, die für bestimmte Prüfungen eingesetzt werden (die „**Screening-Unterauftragsverarbeiterliste**"). Diese Liste kann je nach Zeitpunkt und Umfang der Bestellung des Verantwortlichen variieren.

Aufgrund der kommerziell sensiblen Natur der Bezugs- und Beschaffungsbeziehungen des Auftragsverarbeiters wird die Screening-Unterauftragsverarbeiterliste als vertrauliche Information behandelt und dem Verantwortlichen auf Anfrage zugänglich gemacht, vorbehaltlich von Vertraulichkeitsverpflichtungen, die nicht weiter gehen als jene, die bereits nach dem Hauptvertrag gelten.

Unterauftragsverarbeiter auf der Screening-Unterauftragsverarbeiterliste werden ausschliesslich dann eingesetzt, wenn die jeweilige Informationsquelle die Daten nicht direkt an den Auftragsverarbeiter bereitstellen kann oder wenn keine direkte Quelle existiert. Die Standardpraxis des Auftragsverarbeiters besteht darin, Informationen – soweit technisch und operativ möglich – direkt an der Quelle zu verifizieren, einschliesslich offizieller Register, öffentlicher Behörden

und ausstellender Institutionen. Daher stellt der Einsatz von Unterauftragsverarbeitern zu Verifizierungszwecken die Ausnahme und nicht die übliche Form der Leistungserbringung dar.

Der Auftragsverarbeiter stellt sicher, dass jeder Unterauftragsverarbeiter an Datenschutzpflichten gebunden ist, die – soweit auf die von diesem Unterauftragsverarbeiter erbrachten Dienstleistungen anwendbar – mindestens ebenso schützend sind wie die in diesem Nachtrag festgelegten Verpflichtungen. Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der Datenschutzpflichten jedes Unterauftragsverarbeiters verantwortlich.

8. Grenzüberschreitende Übermittlung

8.1. Grenzüberschreitende Übermittlung an den Auftragsverarbeiter

Befindet sich der Auftragsverarbeiter in einem Land, für das keine Angemessenheitsentscheidung des Schweizer Datenschutzbeauftragten oder keine EU-Angemessenheitsentscheidung vorliegt, vereinbaren die Parteien, die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern (Durchführungsbeschluss (EU) 2021/914 der Kommission) in dieser Vereinbarung aufzunehmen in der von der Europäischen Kommission angenommenen Form, da diese Standardvertragsklauseln von Zeit zu Zeit geändert oder ersetzt werden können (die "**Musterklauseln**").

8.2. Grenzüberschreitende Übermittlung an Unterauftragsverarbeiter

Der Auftragsverarbeiter kann mit vorheriger schriftlicher Zustimmung (einschliesslich per E-Mail und im Tool des Auftragsverarbeiters) des Verantwortlichen gemäss Abschnitt 6 oben personenbezogene Daten in den folgenden Situationen an einen Unterauftragsverarbeiter in einem Land ausserhalb des Europäischen Wirtschaftsraums (EWR), des Vereinigten Königreichs oder der Schweiz übermitteln:

- Übermittlung in ein Land, Gebiet oder einen Sektor, für das bzw. den die Europäische Gemeinschaft und die Schweiz derzeit ein angemessenes Schutzniveau in Bezug auf den Datenschutz festgestellt haben;
- sofern keine Feststellung der Angemessenheit vorliegt, ermächtigt und weist der Verantwortliche den Auftragsverarbeiter hiermit ausdrücklich an, mit dem Unterauftragsverarbeiter mit Sitz in einem Land ausserhalb des EWR, dem Vereinigten Königreich oder der Schweiz im Namen und im Auftrag des Verantwortlichen die Musterklauseln zu unterzeichnen, wobei alle zusätzlichen Anforderungen zu berücksichtigen sind, die von einer zuständigen Datenschutzaufsichtsbehörde und/oder einem zuständigen Gericht auferlegt werden können (wobei der Auftragsverarbeiter dem Verantwortlichen garantiert, dass jede solche Übermittlung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzvorschriften erfolgt, wie sie von den zuständigen Datenschutzaufsichtsbehörden und den zuständigen Gerichten jeweils ausgelegt werden);
- vom Auftragsverarbeiter gleichwertige Massnahmen zur Einhaltung der geltenden Datenschutzvorschriften (gemäss Auslegung durch die zuständigen Datenschutzaufsichtsbehörden und Gerichte) getroffen wurden, um sicherzustellen, dass die Übermittlung personenbezogener Daten in voller Übereinstimmung mit diesen Vorschriften erfolgt; und
- eine solche Übermittlung nach dem Recht der Europäischen Union, der Schweiz, des Vereinigten Königreichs oder dem nationalen Recht, dem der Auftragsverarbeiter unterliegt, zwingend vorgeschrieben ist. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Übermittlung über diese gesetzliche Anforderung, es sei denn, das geltende Recht der Europäischen Union, der Schweiz, des Vereinigten Königreichs

oder das nationale Recht verbietet eine solche Information aus wichtigen Gründen des öffentlichen Interesses.

Wenn einer der oben genannten Mechanismen für die grenzüberschreitende Übermittlung personenbezogener Daten von einer zuständigen Behörde und/oder gemäss den geltenden Datenschutzvorschriften als ungültiges Mittel zur Einhaltung der Beschränkungen für die Übermittlung personenbezogener Daten ausserhalb des EWR, Vereinigtes Königreich oder die Schweiz gemäss den geltenden Datenschutzvorschriften als ungültiges Mittel zur Einhaltung der Beschränkungen für die Übermittlung personenbezogener Daten ausserhalb des EWR, des Vereinigten Königreichs oder der Schweiz angesehen wird, verhandeln die Parteien in gutem Glauben über die Umsetzung einer alternativen Lösung, damit die Partei, die die personenbezogenen Daten übermittelt, die Bestimmungen der geltenden Datenschutzbestimmungen in Bezug auf eine solche Übermittlung einhalten kann.

9. Bereitstellung von Informationen für das Datensubjekt

Der Verantwortliche stellt den betroffenen Personen die gemäss den geltenden Datenschutzbestimmungen erforderlichen Informationen zur Verfügung.

Wenn eine betroffene Person den Auftragsverarbeiter kontaktiert, um eines ihrer Rechte auszuüben, leitet der Auftragsverarbeiter diese Anfrage (und alle anderen relevanten Informationen) unverzüglich an den Verantwortlichen weiter. Sofern der Verantwortliche keine schriftliche Anweisung erteilt hat, antwortet der Auftragsverarbeiter nicht direkt auf eine Anfrage einer betroffenen Person. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage bei der Bearbeitung von Anfragen betroffener Personen gemäss den geltenden Datenschutzbestimmungen. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage bei der Bearbeitung von Anfragen betroffener Personen gemäss den geltenden Datenschutzbestimmungen.

10. Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten

Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 48 Stunden, nachdem er Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erhalten hat.

Die Benachrichtigung enthält, soweit zu diesem Zeitpunkt verfügbar:

- eine Beschreibung der Art der Verletzung (einschliesslich der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze, sofern möglich);
- die wahrscheinlichen Folgen der Verletzung;
- die Massnahmen, die zur Behebung der Verletzung und zur Minderung möglicher nachteiliger Auswirkungen ergriffen oder vorgeschlagen wurden; und
- die Kontaktdaten der für die Reaktion auf Vorfälle zuständigen Kontaktstelle des Auftragsverarbeiters.

Der Auftragsverarbeiter hält den Verantwortlichen über wesentliche Entwicklungen auf dem Laufenden und arbeitet in gutem Glauben mit, damit der Verantwortliche seinen Melde- und Kommunikationspflichten nachkommen kann.

Mitteilungen gemäss diesem Abschnitt sind zu richten an: gdpr@validato.com und info@validato.com.

11. Unterstützung des Verantwortlichen durch den Auftragsverarbeiter

Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen (i) bei Untersuchungen, die von den zuständigen Datenschutzaufsichtsbehörden eingeleitet wurden, oder bei vorherigen

Konsultationen mit diesen Behörden, (ii) bei der Meldung einer Datenschutzverletzung an die Aufsichtsbehörden und der Unterrichtung der betroffenen Personen und (iii) bei der Erstellung einer Datenschutz-Folgenabschätzung zu unterstützen.

Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen alle Informationen und Unterlagen zur Verfügung zu stellen, die erforderlich sind, damit der Verantwortliche die Einhaltung seiner Verpflichtungen gemäss den geltenden Datenschutzvorschriften nachweisen kann.

Der Auftragsverarbeiter gestattet dem Verantwortlichen oder einem vom Verantwortlichen beauftragten Dritten, den Auftragsverarbeiter zu auditieren und zu inspizieren. Ausser in Notfällen (z. B. im Zusammenhang mit einer Anfrage einer zuständigen Aufsichtsbehörde oder im Falle einer Verletzung des Schutzes personenbezogener Daten) darf ein Audit nur während der normalen Arbeitszeiten und nach einer schriftlichen Ankündigung von mindestens 10 (zehn) Tagen durchgeführt werden. Der Umfang des Audits beschränkt sich auf Angelegenheiten, die für diese Vereinbarung relevant sind. Der Verantwortliche trägt die Kosten für jede Prüfung. Wenn bei einer Prüfung festgestellt wird, dass der Auftragsverarbeiter gegen eine seiner Verpflichtungen aus dieser Vereinbarung verstossen hat, wird der Auftragsverarbeiter den Verstoss unverzüglich auf eigene Kosten beheben.

12. Rückgabe/Vernichtung der personenbezogenen Daten

Nach Ablauf des Hauptvertrags muss der Auftragsverarbeiter, sofern keine für ihn geltende zwingende gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, die personenbezogenen Daten innerhalb von 120 Tagen nachweisbar und in Übereinstimmung mit den geltenden Datenschutzbestimmungen sicher löschen.

Der Auftragsverarbeiter bestätigt dem Verantwortlichen schriftlich, dass er keine Kopie der personenbezogenen Daten aufbewahrt hat, es sei denn, der Auftragsverarbeiter ist gesetzlich verpflichtet, eine Kopie der personenbezogenen Daten aufzubewahren. In diesem Fall verpflichtet sich der Auftragsverarbeiter, dass:

- die Vertraulichkeit aller dieser personenbezogenen Daten gewährleistet ist und
- diese personenbezogenen Daten nur so lange verarbeitet werden, wie es für die Zwecke erforderlich ist, die in der gesetzlichen Verpflichtung zur Speicherung festgelegt sind.

13. Aufzeichnung der Datenverarbeitungsaktivitäten

Der Auftragsverarbeiter führt gemäss Artikel 30 Absatz 2 DSGVO und Artikel 12 DSG Aufzeichnungen über die im Auftrag des Verantwortlichen durchgeführten Datenverarbeitungsaktivitäten.

14. Vom Auftragsverarbeiter zu implementierende Sicherheitsmassnahmen

Der Auftragsverarbeiter verpflichtet sich, alle geeigneten technischen und organisatorischen Sicherheitsmassnahmen zu ergreifen, die gemäss Artikel 32 DSGVO und Artikel 8 DSG (sofern anwendbar) erforderlich sind und in Anhang B (die "**Sicherheitsmassnahmen**") aufgeführt sind, um ein den Risiken angemessenes Sicherheitsniveau zu gewährleisten, einschliesslich, falls erforderlich:

- ein Verfahren zur Gewährleistung der fortlaufenden Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und Dienste;
- ein Verfahren zur zeitnahen Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls;

- ein Verfahren zur regelmässigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung;
- Massnahmen zur Gewährleistung, dass jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, die personenbezogenen Daten ausschliesslich gemäss den Weisungen des Verantwortlichen verarbeitet; und
- alle anderen in dieser Vereinbarung oder in den Anweisungen des Verantwortlichen festgelegten Massnahmen.

Der Auftragsverarbeiter muss die Sicherheitsmassnahmen aufrechterhalten und regelmässig überprüfen, um sicherzustellen, dass diese Massnahmen aktuell, wirksam und angemessen sind, was die Sensibilität der personenbezogenen Daten betrifft.

Der Auftragsverarbeiter nimmt an einem Zertifizierungsmechanismus teil (gemäss Artikel 13 DSG oder Artikel 42 DSGVO (falls zutreffend)). Der vom Auftragsverarbeiter verwendete Zertifizierungsmechanismus ist ISO 27001.

Für die Dauer des Hauptvertrags verpflichtet sich der Auftragsverarbeiter, die relevanten Anforderungen seiner ISO 27001-Zertifizierung kontinuierlich zu erfüllen und diese Zertifizierung vor ihrem Ablauf zu erneuern. Auf Anfrage legt der Auftragsverarbeiter dem Verantwortlichen einen Nachweis über die gültige ISO 27001-Zertifizierung vor. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn die ISO 27001-Zertifizierung nicht erneuert wird, ohne Erneuerung abläuft, ausgesetzt oder widerrufen wird.

15. Rollen des Verantwortlichen und des Auftragsverarbeiters

Für alle personenbezogenen Daten, die gemäss dieser Vereinbarung im Zusammenhang mit den Diensten (einschliesslich Überprüfungen/Hintergrundüberprüfungen) verarbeitet werden, ist der Verantwortliche der Verantwortliche und der Auftragsverarbeiter der Auftragsverarbeiter.

Der Auftragsverarbeiter kann begrenzte geschäftliche Kontaktdaten der autorisierten Benutzer und Vertreter des Verantwortlichen (z. B. Name, geschäftliche E-Mail-Adresse, Telefonnummer, Funktion, Rechnungs- und Supportkommunikation) als unabhängiger Verantwortlicher für Zwecke der Kontoverwaltung, Rechnungsstellung, Betrugsbekämpfung und Compliance verarbeiten. Diese Verarbeitung unterliegt der Datenschutzerklärung des Auftragsverarbeiters und dem geltenden Recht.

16. Gerichtsbarkeit und anwendbares Recht

Die im Hauptvertrag festgelegte Gerichtsstandsklausel gilt auch für diese Vereinbarung.

Die im Hauptvertrag festgelegte Rechtswahlklausel gilt auch für diese Vereinbarung.

ANHANG A – Kategorien personenbezogener Daten

Identifikationsdaten

- Vorname
- Nachname
- Geburtsdatum und -ort
- Staatsangehörigkeit
- Wohnsitz
- Amtliche Vormundschaft
- Zivilstatus
- Vor- und Nachname der Eltern
- Personalausweis
- Reisepass
- E-Mail-Adresse
- Telefonnummer
- Alter
- Geschlecht
- Arbeitserlaubnisse
- Nationale Identifikationsnummer
-

KYC-Daten

- Berufliche Tätigkeit
- Öffentliche Funktionen (lokale und internationale PEP, internationale und Sportorganisationen usw.)
- Auszug aus dem Strafregister
- Inkassoregister/finanzielle Integrität
- persönliche Bonität

Gewohnheits- und Beziehungsdaten

- Freizeitaktivitäten
- besonderes Verhalten oder soziale Kontakte
- Familie und eingetragene Partnerschaft
- Mitgliedschaften in Vereinigungen (ausser im Bereich Politik, Religion oder Gewerkschaften)

Karrierebezogene Daten

- CV
- Arbeitszeugnisse
- Abschlüsse
- Referenzen
- externe Mandate
- Vertretungsbefugnisse

Daten zu persönlichen Merkmalen

- politische Meinungen

Biometrische Daten

- Gesichtsscan der betroffenen Person, einschliesslich Live-Erfassung aus mehreren Blickwinkeln

ANHANG B – Sicherheitsmassnahmen

1. Governance & Richtlinien

- Informationssicherheitsrichtlinien, Risikomanagement und regelmässige Überprüfungen.
- Vertraulichkeitspflichten für Mitarbeiter und Auftragnehmer.

2. Zugriffskontrolle

- Rollenbasierte Zugriffskontrolle (geringstmögliche Berechtigungen), MFA für administrativen Zugriff.
- Starke Authentifizierung, sichere Passwortrichtlinien, regelmässige Zugriffsüberprüfungen.

3. Verschlüsselung

- Verschlüsselung während der Übertragung (TLS) und Verschlüsselung im Ruhezustand für gespeicherte personenbezogene Daten, sofern zutreffend.
- Kontrollen der Schlüsselverwaltung und eingeschränkter Zugriff auf Schlüssel.

4. Protokollierung und Überwachung

- Sicherheitsprotokolle für Zugriff und administrative Massnahmen.
- Überwachung/Warnung bei verdächtigen Aktivitäten.

5. Schwachstellen- und Patch-Management

- Regelmässige Schwachstellenscans und zeitnahe Sicherheitspatches.
- Sichere Konfigurationsbasislinien.

6. Sichere Entwicklung und Änderungsmanagement (falls zutreffend)

- Änderungskontrolle, Peer-Review, Trennung von Umgebungen.
- Risikogerechte Sicherheitstests.

7. Sicherung und Wiederherstellung

- Regelmässige Sicherungen, sofern zutreffend; Wiederherstellungstests.
- Risikogerechte Massnahmen zur Notfallwiederherstellung und Geschäftskontinuität.

8. Reaktion auf Sicherheitsvorfälle

- Dokumentierter Prozess zur Reaktion auf Vorfälle; Eskalationswege bei Verstössen.
- Überprüfung nach Vorfällen und Korrekturmassnahmen.

9. Sicherheit von Unterauftragsverarbeitern

- Sorgfaltspflicht und vertragliche Sicherheitsverpflichtungen; Überwachung der Einhaltung.

10. Datenminimierung und -aufbewahrung

- Logische Trennung zwischen Kunden; Aufbewahrungskontrollen gemäss Ziffer 11.