Anlage 7 zum Vertrag DAL Bautec - Alasco

DATENVEREINBARUNG

ZUM VERTRAG ÜBER DIE BEREITSTELLUNG EINER WEB-BASIERTEN SOFTWARELÖSUNG FÜR DIGITALISIERTE PROZESSE IM RAHMEN DES KOSTENCONTROLLINGS BEI DER DURCHFÜHRUNG VON BAUPROJEKTEN

ZUR AUFTRAGSVERARBEITUNG

(ART. 28 (3) DS-GVO)

(STAND: OKTOBER 2020)

PRÄAMBEL

Der Auftraggeber (“Kunde”) und der Auftragnehmer (“Alasco GmbH”) haben einen Vertrag über die Bereitstellung einer webbasierten Softwarelösung für digitalisierte Prozesse im Rahmen des Finanzcontrollings bei der Durchführung von Bauprojekten ("Vertrag") abgeschlossen.

Im Rahmen der Ausübung der Pflichten des Vertrags verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers in Übereinstimmung mit Art. 28 der Datenschutz-Grundverordnung 2016/679 gemäß den hierin und im Vertrag festgelegten Vorgaben ("Auftragsverarbeitung").

Dieser Annex regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung.

Vor diesem Hintergrund vereinbaren die Parteien daher Folgendes:

1. DEFINITIONEN

Begriffe, die in diesem Annex verwendet werden, haben die Bedeutung der Begriffe des Vertrags oder dieser Anlage. Sofern nicht abweichend geregelt, gelten die Begriffsbestimmungen der EU Datenschutz-Grundverordnung 2016/679 ("DS-GVO"), insbesondere für die Begriffe "Verantwortlicher", "betroffene Person", "Mitgliedstaat", "personenbezogene Daten", "Verletzung des Schutzes personenbezogener Daten", "Auftragsverarbeiter", "Verarbeitung" und "Aufsichtsbehörde".

2. GEGENSTAND DES ANNEX

2.1 Der Auftragnehmer verarbeitet Auftraggeberdaten zum Zweck der Erbringung der im Vertrag beschriebenen Dienstleistungen ("Auftragsdienstleistungen") sowie weitere Dienstleistungen gemäß dieses Annex ("Verarbeitungsdienstleistungen") für den Auftraggeber ("zulässiger Zweck"). „Auftraggeberdaten“ steht für alle durch den Auftragnehmer im Auftrag des Auftraggebers gemäß oder in Verbindung mit dem Hauptvertrag verarbeiteten personenbezogene Daten.

Die Parteien stimmen überein, dass im Rahmen der Verarbeitung von Auftraggeberdaten gemäß diesem Annex der Auftraggeber als Verantwortlicher und der Auftragnehmer als Auftragsverarbeiter tätig werden.

2.2 Sub-Annex 1 regelt die Details der

(a) Zwecke der Verarbeitung;

(b) Kategorien der Auftraggeberdaten;

(c) Kategorien der von der Verarbeitung betroffenen Personen.

2.3 Die Verarbeitung findet zu jeder Zeit auf professionelle Weise und im Einklang mit den Grundsätzen einer angemessenen Datenverarbeitung, den Vorschriften des Vertrags, dieses Annex und des anwendbaren Rechts statt.

2.4 Soweit der Auftragnehmer Auftraggeberdaten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums "EWR" verarbeitet oder die Verarbeitung von Auftraggeberdaten dem Recht von Staaten außerhalb der Europäischen Union bzw. des EWR unterliegt, wird der Auftragnehmer die anwendbaren datenschutzrechtlichen Gesetze einhalten, insbesondere geeignete Schutzmaßnahmen ergreifen, um ein angemessenes Datenschutzniveau im Einklang mit Art. 44ff. DS-GVO zu gewährleisten.

2.5 Für den Fall, dass die EU Kommission oder eine zuständige Aufsichtsbehörde Standardvertragsklauseln gemäß Art. 28 Abs. 7 DS-GVO festlegt, ergänzen die Parteien auf Verlangen einer Partei diesen Annex unverzüglich um diese Vertragsklauseln, wenn dies zur Einhaltung anwendbaren Rechts erforderlich ist. Dasselbe gilt für alle anderen Änderungen anwendbaren Rechts, die eine Anpassung dieses Annex erfordern.

3. WEISUNGEN DES AUFTRAGGEBERS

3.1 Der Auftragnehmer verarbeitet Auftraggeberdaten zum Zweck der Verarbeitungsdienstleistungen ausschließlich im Auftrag und nach den dokumentierten Weisungen des Auftraggebers. Das gilt auch für Weisungen hinsichtlich der Übermittlung an ein Drittland oder eine internationale Organisation, sofern der Auftragnehmer hierzu nicht durch ein Gesetz der Europäischen Union oder eines Mitgliedstaats verpflichtet ist. In diesem Fall setzt der Auftragnehmer den Auftraggeber, sofern nicht gesetzlich untersagt, unverzüglich vor Beginn der Verarbeitung schriftlich über die gesetzliche Verpflichtung in Kenntnis. Regelungen hinsichtlich der Verarbeitung von Auftraggeberdaten in diesem Annex oder im Vertrag (z.B. eine Verpflichtung zur Anonymisierung bestimmter personenbezogener Daten des Auftraggebers) gelten als Weisung des Auftraggebers gemäß dieses Annex.

"Drittland" steht für Staaten, die nicht Mitglieder der EU oder des EWR sind und von der Europäischen Kommission nicht als Staaten anerkannt sind, die einen angemessenen Grad an Schutz für personenbezogene Daten gewährleisten.

3.2 Falls eine Anweisung des Auftraggebers einer Verpflichtung des Auftragnehmers nach dem Vertrag oder dieses Annex entgegensteht oder anderweitig negative Auswirkungen auf die Auftragsdienstleistungen hat, werden sich die Parteien gemeinsam auf angemessene Änderungen des Vertrags einigen. Der Auftraggeber stellt den Auftragnehmer vollumfänglich frei von jeglichen Kosten, Ansprüchen, Schäden, Strafen und sonstiger Verbindlichkeiten (einschließlich angemessener Kosten für die Untersuchung und Verteidigung sowie angemessene Anwaltskosten und anderer Beraterkosten), die aus der Umsetzung einer solchen Anweisung resultieren. Der Auftraggeber wird dem Auftragnehmer unverzüglich nach Rechnungsstellung durch den Auftragnehmer jegliche zusätzlichen Kosten und Auslagen vergüten, die dem Auftragnehmer aufgrund der Umsetzung derartiger Anweisungen entstanden sind.

4. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

4.1 Der Auftragnehmer wird für die Dauer der Auftragsverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme im Einklang mit diesem Annex sicherstellen. Im Falle einer technischen Störung oder anderen Beeinträchtigungen wird der Auftragnehmer schnellstmöglich nach besten Kräften Verfügbarkeit und Zugriff auf die Auftraggeberdaten wiederherstellen.

Der Auftragnehmer ist verpflichtet, alle unter Berücksichtigung des Stands der Technik, der Implementierungskosten und von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, angemessenen technischen und organisatorischen Maßnahmen zu treffen, um

(a) unberechtigte oder widerrechtliche Verarbeitung, Verlust, Zerstörung oder Beschädigung von Auftraggeberdaten zu verhindern und

(b) ein angemessenes Sicherheitsniveau sicherzustellen unter Berücksichtigung der möglichen Schäden für und der Art der zu schützenden Auftraggeberdaten

einschließlich der in Art. 32 der DS-GVO in Bezug genommenen Maßnahmen ("Datensicherheitsstandards").

4.2 Sub-Annex 2 spezifiziert die vom Auftragnehmer umgesetzten Datensicherheitsstandards.

4.3 Da die Datensicherheitsstandards technischem Fortschritt und technischer Entwicklung unterliegen, ist der Auftragnehmer berechtigt, geeignete alternative technische und organisatorische Maßnahmen zu ergreifen, jedoch dürfen diese Maßnahmen das Sicherheitsniveau der Datensicherheitsstandards nicht unterschreiten und müssen den Anforderungen des anwendbaren Rechts entsprechen.

5. RECHTE DER BETROFFENEN PERSONEN

5.1 Der Auftraggeber ist für die Bearbeitung von Anfragen von betroffenen Personen und die Erfüllung der gesetzlichen Rechte von betroffenen Personen im Zusammenhang mit der Verarbeitung von Auftraggeberdaten verantwortlich. Der Auftragnehmer wird sich nach besten Kräften bemühen, dem Auftraggeber umgehend alle für den Umgang mit Anfragen von betroffenen Personen erforderlichen Informationen zur Verfügung zu stellen.

5.2 Der Auftragnehmer informiert den Auftraggeber umgehend über alle Anfragen von betroffenen Personen oder andere Fragen im Zusammenhang mit diesem Annex und beantwortet derartige Anfragen oder Fragen nur auf ausdrückliche dokumentierte Weisung durch den Auftraggeber.

5.3 Bei Streitigkeiten einer oder beider Parteien mit betroffenen Personen oder mit von betroffenen Personen geltend gemachten Ansprüchen bezüglich der Verarbeitung der Auftraggeberdaten, werden die betroffenen Parteien sich umgehend gegenseitig benachrichtigen und unterrichten und hinsichtlich einer effektiven Verteidigung gegen solche Ansprüche oder einer gütlichen Einigung zeitnah zusammenarbeiten und sich absprechen.

6. WEITERE DATENSCHUTZRECHTLICHE PFLICHTEN

6.1 Der Auftragnehmer führt ein ordnungsgemäß dokumentiertes (wobei die elektronische Form ausreichend ist) Verzeichnis der im Auftrag des Auftraggebers durchgeführten Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO.

6.2 Der Auftragnehmer leistet dem Auftraggeber angemessene Unterstützung bei

(a) der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO für die Auftragsverarbeitung; auf Aufforderung durch den Auftraggeber stellt er dem Auftraggeber unverzüglich alle für diesen Zweck erforderlichen Informationen in einem geeigneten Format zur Verfügung;

(b) der Datenschutz-Folgeabschätzung gemäß Art. 35 DS-GVO; und

(c) Anfragen oder Verfahren der zuständigen Aufsichtsbehörde.

7. PERSONAL DES AUFTRAGNEHMERS / DATENSCHUTZBEAUFTRAGTER

7.1 Der Auftragnehmer stellt sicher, dass das bei der Auftragsverarbeitung eingesetzte Personal über geeignete Qualifikation und Ausbildung (einschließlich einer angemessenen spezifischen Datenschutzschulung) verfügt und sich verpflichtet hat, die Auftraggeberdaten vertraulich zu behandeln bzw. einer angemessenen gesetzlichen Vertraulichkeitsverpflichtung unterliegt, welche nach Beendigung dieses Annex fort gilt.

7.2 Soweit nach anwendbarem Recht erforderlich, bestellt der Auftragnehmer einen Datenschutzbeauftragten und teilt dem Auftraggeber unverzüglich dessen aktuelle Kontaktinformationen mit.

8. UNTERAUFTRAGSVERHÄLTNISSE

8.1 Der Auftragnehmer wird hiermit ermächtigt, nach Maßgabe des anwendbaren Rechts weitere Auftragsverarbeiter im Zusammenhang mit der Auftragsverarbeitung von Auftraggeberdaten ("Subunternehmer") zu beauftragen. Ziffer 2.3 findet auf die Verarbeitung von Auftraggeberdaten durch einen Subunternehmer in einem Drittstaat entsprechende Anwendung. Der Auftraggeber stimmt insbesondere der Beauftragung von mit dem Auftragnehmer verbundenen Unternehmen und der in Sub-Annex 3 aufgeführten tatsächlichen oder potentiellen Subunternehmer zu. Der Auftraggeber ergreift unverzüglich alle angemessenen erforderlichen oder geeigneten Handlungen, um die Übermittlung von Auftraggeberdaten an genehmigte Subunternehmer zu erleichtern oder zu unterstützen (bspw. durch die Aktualisierung von Registrierungen bei den Datenschutzbehörden).

8.2 Der Auftragnehmer führt (derzeit abrufbar unter https://www.alasco.de/liste-der-subunternehmer/) eine aktuelle Liste der derzeit von Alasco beauftragten Subunternehmen. Mindestens 30 Tage bevor der Auftragnehmer einen neuen Subunternehmer mit der Durchführung von Verarbeitungsaktivitäten von Auftraggeberdaten beauftragt, aktualisiert Alasco die entsprechende Webseite und stellt dem Auftraggeber einen Mechanismus zur Verfügung, um eine Benachrichtigung über diese Aktualisierung zu erhalten. Der Auftraggeber kann der Beauftragung innerhalb von 30 Tagen nach Erhalt der Mitteilung durch schriftliche Mitteilung an den Auftragnehmer aus berechtigten Gründen widersprechen. Im Fall eines Widerspruchs aus berechtigten Gründen wird der Auftragnehmer entscheiden, welche zumutbaren Maßnahmen ergriffen werden können, um zu verhindern, dass der betreffende Subunternehmer Auftraggeberdaten verarbeitet oder die berechtigten Gründe für den Widerspruch anderweitig zu beheben ohne den Auftragnehmer unangemessen zu belasten. Wenn der Auftragnehmer solche Anpassungen nicht innerhalb eines angemessenen Zeitraums, der dreißig (30) Tage nicht überschreiten darf, umsetzen kann, ist der Auftraggeber berechtigt, schriftlich unter Einhaltung einer

Kündigungsfrist von dreißig (30) Tagen nach der Entscheidung des Auftragnehmers über die Maßnahme zur Abhilfe diejenigen Auftragsdienstleistungen zu kündigen, die vom Auftragnehmer nicht ohne Einsatz des betreffenden Subunternehmers erbracht werden können.

Berechtigte Gründe liegen nur dann vor, wenn objektive Tatsachen die Vermutung stützen, dass die Beauftragung des Subunternehmers gegen anwendbares Recht oder diesen Annex verstoßen würde.

8.3 Wenn der Auftragnehmer einen Subunternehmer mit der Durchführung bestimmter Verarbeitungsaktivitäten im Auftrag des Auftraggebers beauftragt, trifft der Auftragnehmer eine schriftliche Vereinbarung mit dem Subunternehmer, die für die Auftraggeberdaten wenigstens das gleiche Schutzniveau bietet, wie in diesem Annex festgelegt und die Anforderungen von Art. 28 Abs. 3 DS-GVO erfüllt. Die Vereinbarung mit dem Subunternehmer umfasst ein direktes Prüfungsrecht für den Auftraggeber oder andere geeignete Prüfungsmechanismen (bspw. Prüfungen durch Dritte oder Prüfungen, die im Auftrag des Auftraggebers durch den Auftragnehmer durchgeführt werden).

8.4 Zur Sicherstellung, dass der Subunternehmer die Datensicherheitsstandards, anwendbares Recht und seine weiteren vertraglichen Verpflichtungen erfüllt, führt der Auftragnehmer regelmäßige Prüfungen gemäß anwendbarem Recht durch.

8.5 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage stets eine aktuelle Liste der Subunternehmer mit Angaben zur Firma, der Adresse, der konkreten ausgelagerten Auftragsverarbeitung und dem Ort der Verarbeitung zur Verfügung.

8.6 Falls der Subunternehmer eine vertragliche Verpflichtung in schwerwiegender Weise verletzt und dadurch die Sicherheit und Integrität der Auftraggeberdaten gefährdet, haftet der Auftragnehmer dem Auftraggeber vollumfänglich für alle Schäden, die durch diese Verletzung entstehen und stellt den Auftraggeber diesbezüglich von allen Ansprüchen im Zusammenhang mit oder infolge der Beauftragung des Subunternehmers frei.

9. ÜBERMITTLUNG IN DRITTLÄNDER

9.1 Soweit die Verarbeitung von Auftraggeberdaten in einem Drittland erfolgt oder die Gesetze einer anderen Rechtsordnung Anwendung finden, befolgt der Auftragnehmer die anwendbaren Gesetze, insbesondere ergreift er angemessene Garantien zur Sicherstellung eines ausreichenden Datenschutzniveaus im Einklang mit Art. 44 f. DS-GVO.

9.2 Die Parteien werden vor jeder Übermittlung von Auftraggeberdaten alle gemäß anwendbarem Recht notwendigen Vereinbarungen treffen und sonstige Handlungen vornehmen, insbesondere die Standardvertragsklauseln gemäß der Kommissionsentscheidung vom 5. Februar 2010 (2010/87/EU) sowie andere nach anwendbarem Recht erforderliche Instrumente vereinbaren. Sofern nach anwendbarem Recht erforderlich, stellt der Auftragnehmer sicher, dass auch mit allen Subunternehmern entsprechende Instrumente oder Verpflichtungen vereinbart werden.

10. INSPEKTIONEN UND PRÜFUNGEN

10.1 Der Auftragnehmer stellt dem Auftraggeber unverzüglich auf dessen Anforderung alle erforderlichen Informationen zur Verfügung, um die Einhaltung dieses Annex zu dokumentieren. Der Auftraggeber ist berechtigt, Überprüfungen im Zusammenhang mit der Verarbeitung von Auftraggeberdaten, einschließlich von Inspektion der Datenverarbeitungseinrichtungen des Auftragnehmers vor Ort, entweder selbst oder durch einen gemäß dieser Ziffer benannten Prüfer durchzuführen. Der Auftragnehmer wird insoweit mitwirken und unterstützen.

10.2 Der Auftragnehmer stellt dem Auftraggeber unverzüglich auf dessen Anforderung eine Zusammenfassung der Ergebnisse seiner letzten internen Datensicherheitsprüfung zur Verfügung. Außerdem wird der Auftragnehmer, auf Verlangen des Auftraggebers und nicht mehr als einmal pro Jahr, an einer schriftlichen Informationssicherheitsbefragung durch den Auftraggeber teilnehmen, welche die Einhaltung der Datensicherheitsstandards seitens des Auftragnehmers bewertet.

10.3 Informations- und Prüfungsrechte des Auftraggebers gemäß Ziffer 10.1 erwachsen nur falls und insoweit (i) der Vertrag Informations- und Prüfungsrechte nicht anderweitig unter Einhaltung der jeweiligen Anforderungen des

anwendbaren Rechts (einschließlich Art. 28 Abs. 3 (h) DS-GVO) regelt und (ii) die gemäß Ziffer 10.2 zur Verfügung gestellten Informationen nicht ausreichen, damit der Auftraggeber seinen Inspektion- und Prüfungspflichten nach anwendbarem Recht nachkommen kann.

10.4 Der Auftraggeber wird dem Auftragnehmer eine durchzuführende Prüfung oder Inspektion mindestens drei (3) Wochen im Voraus anzeigen und wird vermeiden, dass dabei Schäden, Beeinträchtigungen oder Störungen verursacht werden. Der Auftragnehmer muss zum Zweck einer solchen Prüfung oder Inspektion keinen Zutritt gewähren:

(a) Personen, die keinen angemessenen Nachweis ihrer Identität und Befugnis vorlegen;

(b) für die Zwecke von mehr als einer Prüfung oder Inspektion pro Kalenderjahr, mit der Ausnahme von zusätzlichen Prüfungen und Inspektionen, welche der Auftraggeber aufgrund Aufforderung einer Aufsichtsbehörde oder anderen zuständigen Behörde durchzuführen hat.

10.5 Wenn der Auftraggeber Mängel oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung von Auftraggeberdaten feststellt und diese dem Auftragnehmer schriftlich anzeigt, werden Auftragnehmer und Auftraggeber gemeinsam ein beiderseitig zufriedenstellendes Konzept zu deren Behebung erarbeiten.

10.6 Das Kopieren und die Entfernung von Dokumenten oder Informationen aus den Räumlichkeiten des Auftragnehmers ist ohne die vorherige schriftliche Einwilligung des Auftragnehmers nicht gestattet. Alle nichtöffentlichen Dokumente und Informationen, die dem Auftraggeber gemäß dieser Ziffer gegenüber offengelegt werden, gelten als geschützte und vertrauliche Informationen des Auftragnehmers. Der Auftraggeber legt keine solchen Dokumente oder Informationen gegenüber Dritten offen oder nutzt sie für andere Zwecke als die Bewertung der Einhaltung der Datensicherheitsstandards durch den Auftragnehmer.

10.7 Soweit nach anwendbarem Recht Anpassungen der vorstehenden Prüfungsrechte erforderlich sind oder werden, wird dieser Annex so ausgelegt bzw. angepasst, dass sie diesen zusätzlichen gesetzlichen Anforderungen genügt. Der Auftragnehmer setzt den Auftraggeber unverzüglich in Kenntnis, wenn eine Weisung gemäß dieser Ziffer nach seiner Auffassung gegen EU Datenschutzgesetze oder andere Datenschutzvorschriften von Mitgliedstaaten verstößt (Art. 28 Abs. 3 DS-GVO).

11. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

11.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich über alle tatsächlichen oder vermutlichen technischen, organisatorischen oder sonstigen Vorfälle, die zu einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 33 Abs. 1 DS-GVO führen oder anderweitige nachteilige Auswirkungen auf die Integrität und Sicherheit von Auftraggeberdaten oder die Auftragsverarbeitung haben ("Datensicherheitsvorfall").

Datensicherheitsvorfälle umfassen insbesondere die Folgenden:

(a) tatsächlicher oder vermutlicher unberechtigter Zugriff, Offenlegung, Verlust, Download, Diebstahl, Sperrung, Kodierung oder Löschung durch Malware oder sonstige unberechtigte Handlungen im Zusammenhang mit Auftraggeberdaten;

(b) Betriebsvorfälle, die eine Auswirkung auf die Verarbeitung der Auftraggeberdaten haben können;

(c) tatsächliche oder vermutliche Verstöße gegen diesen Annex oder anwendbares Recht durch den Auftragnehmer, seine Mitarbeiter oder sonstige Erfüllungsgehilfen, sofern ein solcher Verstoß Auftraggeberdaten oder die Verpflichtungen des Auftragnehmers gemäß diesem Annex betrifft; oder

(d) rechtlich bindende Offenlegungsverlangen oder Beschlagnahmen von Auftraggeberdaten durch Vollstreckungs- oder andere Behörden, sofern es dem Auftragnehmer nicht gesetzlich untersagt ist, dem Auftraggeber einen solchen Vorfall zu melden. In diesem Fall ist der Auftragnehmer verpflichtet, den Auftraggeber unverzüglich zu informieren, sobald dieses Verbot erlischt.

11.2 Die Mitteilung des Auftragnehmers an den Auftraggeber über einen Datensicherheitsvorfall muss umfassend sein und insbesondere alle Informationen enthalten, die gemäß Art. 33 Abs. 3 DS-GVO und/oder gemäß anwendbarem Recht erforderlich sind.

11.3 Die Meldung ist per Telefon und per E-Mail zu richten an die im Angebot angegebene Kontaktadresse.

11.4 Ist der Auftragnehmer gemäß anwendbarem Recht dazu verpflichtet, den Datensicherheitsvorfall an eine Aufsichtsbehörde oder eine andere Behörde, den betroffenen Personen oder anderen Dritten zu melden, wird er vor einer solchen Mitteilung soweit rechtlich zulässig den Auftraggeber informieren. Die Parteien werden sich nach bestem Wissen um einen gemeinsamen Ansatz mit dem Ziel einer Vermeidung von widersprüchlichen oder nicht schlüssigen Meldungen bemühen. Dies umfasst die gegenseitige Bereitstellung der Einzelheiten von Meldungen sowie von Datum und Zeitpunkt, zu dem die Meldung erfolgen wird.

11.5 Im Fall eines Datensicherheitsvorfalls, ergreift der Auftragnehmer umgehend alle erforderlichen und angemessenen Maßnahmen gemäß anwendbarem Recht und technischen Standards, um die Vertraulichkeit, Integrität und Verfügbarkeit der Auftraggeberdaten und die Belastbarkeit der Verarbeitungssysteme und –dienste wiederherzustellen und das Schadenrisiko und alle nachteiligen Auswirkungen für die betroffenen oder potentiell durch den Datensicherheitsvorfall betroffenen Personen zu mindern.

12. KOMMUNIKATION MIT BEHÖRDEN

12.1 Soweit nach anwendbarem Recht zulässig, informiert der Auftragnehmer den Auftraggeber im Fall von Prüfungen, Anfragen, Untersuchungen, Aufforderungen, Anordnungen oder anderen Verfahren oder Angelegenheiten in Bezug auf diesen Annex, durch eine Aufsichtsbehörde oder eine andere Behörde in Bezug auf die Verarbeitung von personenbezogenen Daten ("Behördenanfragen"). Die Parteien bemühen sich nach Kräften, sich gegenseitig zu unterstützen und eine abgestimmte und koordinierte Kommunikation mit der Behörde bezüglich der Behördenanfrage sicherzustellen.

12.2 Im Fall einer Streitigkeit mit einer Aufsichtsbehörde, von Anordnungen derselben oder von derselben auferlegten Geldstrafen oder anderen von einer Aufsichtsbehörde geltend gemachten Ansprüche oder jeweils einer anderen zuständigen Behörde hinsichtlich der Verarbeitung personenbezogener Daten gegen eine oder beide Parteien, werden die Parteien sich umgehend gegenseitig benachrichtigen und unterrichten, und hinsichtlich einer effektiven Verteidigung gegen besagte Ansprüche oder einer gütlichen Einigung zeitnah zusammenarbeiten und sich absprechen.

13. KOSTEN DER VERARBEITUNGSDIENSTLEISTUNGEN

13.1 Sofern nicht ausdrücklich abweichend in diesem Annex oder im Vertrag geregelt, vergütet der Auftraggeber dem Auftragnehmer umgehend nach Rechnungserhalt alle angemessenen aufgetretenen und erforderlichen Kosten und Ausgaben im Zusammenhang mit der Erbringung der Verarbeitungsdienstleistungen gemäß diesem Vertrag (d.h. Dienstleistungen, die über die Auftragsdienstleistungen hinausgehen und die nicht auf rechtlichen Verpflichtungen des Auftragnehmers beruhen).

13.2 Ziffer 13.1 gilt nicht für unwesentliche, einmalige Kosten, die durch die gemäß dem Vertrag zu erstattenden Kosten von den Parteien als abgedeckt betrachtet werden dürfen. Zur Klarstellung: Dies umfasst insbesondere nicht die gemäß den Ziffern 4, 5, 9 und 10 erbrachten Verarbeitungsdienstleistungen.

14. VERPFLICHTUNGEN DES AUFTRAGGEBERS

14.1 Der Auftraggeber ergreift umgehend alle erforderlichen Maßnahmen, um seine eigenen Verpflichtungen nach anwendbarem Recht im Zusammenhang mit der Verarbeitung von Auftraggeberdaten gemäß diesem Annex zu erfüllen und um den Auftragnehmer in zumutbarer Weise bei der der Einhaltung seiner Verpflichtungen zu unterstützen.

14.2 Der Auftraggeber versichert, dass (i) er dazu berechtigt ist, den Auftragnehmer zu beauftragen und dem Auftragnehmer Auftraggeberdaten bereitzustellen und dass (ii) die Verarbeitung der Auftraggeberdaten keine Rechte Dritter verletzt sofern der Auftragnehmer das anwendbare Recht und die Bestimmungen dieses Annex einhält.

15. RÜCKGABE UND LÖSCHPFLICHTEN

15.1 Nach Beendigung des Vertrags oder auf jederzeit mögliches Verlangen des Auftraggebers, löscht der Auftragnehmer umgehend alle Kopien der personenbezogenen Auftraggeberdaten und sorgt für deren Löschung. Sofern und soweit eine Löschung technisch nicht in angemessener Weise umsetzbar ist, stellt der Verarbeiter sicher, dass die personenbezogenen Auftraggeberdaten anonymisiert oder dauerhaft gegenüber unbefugtem Zugriff, unbefugte Offenlegung oder Verwendung gesperrt und geschützt sind. Auf Verlangen des Auftraggebers ist der Auftragnehmer verpflichtet, dem Auftraggeber eine Kopie aller personenbezogenen Auftraggeberdaten mittels sicherer Datenübertragung in einem vom Auftraggeber bestimmten Format zu übermitteln.

15.2 Wenn der Auftraggeber eine Löschung von personenbezogenen Auftraggeberdaten vor Beendigung des Vertrags aus anderen Gründen als einer schwerwiegenden Verletzung wesentlicher Pflichten nach diesem Annex durch den Auftragnehmer vornimmt, wird der Auftraggeber den Auftragnehmer vollumfänglich freistellen hinsichtlich jeglicher Kosten, Ansprüche, Schäden, Strafen und sonstiger Verbindlichkeiten (einschließlich angemessener Kosten für die Untersuchung und Verteidigung sowie angemessene Anwaltskosten und anderer Beraterkosten), die dieser aus Aufforderung resultieren. Diese Freistellungsverpflichtung ist nicht durch Haftungsbeschränkungen oder andere Einschränkungen aus dem Vertrag begrenzt.

15.3 Der Auftragnehmer ist berechtigt, personenbezogene Auftraggeberdaten weiterhin zu speichern wenn, soweit und solange er dazu nach anwendbarem Recht verpflichtet ist, jedoch stets vorausgesetzt, dass der Auftragnehmer sicherstellt, dass die personenbezogenen Auftraggeberdaten (i) vertraulich behandelt werden und vor unberechtigtem Zugriff und Nutzung geschützt sind, und (ii) nur im Rahmen der gesetzlich festgelegten Zwecke der Speicherung verarbeitet werden und nicht für andere Zwecke.

15.4 Auf schriftliche Anforderung des Auftraggebers bestätigt der Auftragnehmer dem Auftraggeber schriftlich, dass er seine Pflichten gemäß dieser Ziffer erfüllt hat.

16. ANONYMISIERUNG

16.1 Der Auftragnehmer hat das Recht, die von dieser Vereinbarung umfassten personenbezogenen Daten zu anonymisieren und zu aggregieren und die für die Anonymisierung und Aggregation erforderlichen Verarbeitungsschritte durchzuführen. Unter Wahrung der Anonymität kann der Auftragnehmer alle so entstandenen Daten für eigene, interne Zwecke (z.B. Produktverbesserungen, Produktentwicklungen) verwenden. Eine selbstständige Weitergabe solcher Daten an Dritte ist ausgeschlossen.

16.2 Anonymisierte oder aggregierte Daten im Sinne von Ziffer 16.1 gelten nicht länger als personenbezogene Daten und werden nicht von der Herausgabe- oder Löschpflicht von Ziffer 15 umfasst. Der Auftragnehmer ist berechtigt, solche Daten für eigene und damit interne Zwecke über das Vertragsende hinaus zu nutzen und aufzubewahren.

17. VERSTOSS GEGEN DIESEN ANNEX

17.1 Im Fall einer Verletzung der Aufgaben und Pflichten des Auftragnehmers aus diesem Annex finden die entsprechenden Bestimmungen der allgemeinen Geschäftsbedingungen des Auftragnehmers Anwendung.

18. DATENSCHUTZRECHTLICH NOTWENDIGE ANPASSUNGEN

18.1 Beide Parteien sind berechtigt, die andere Partei mit einer mindestens zweiwöchigen Frist schriftlich über Änderungen zu diesem Annex zu informieren, die die jeweilige Partei als datenschutzrechtlich notwendig erachtet. Die Parteien stellen daraufhin unverzüglich gemeinsam sicher, dass die datenschutzrechtlich notwendigen Änderungen vorgenommen werden.

18.2 Im Fall von Änderungen des anwendbaren Rechts oder Hinweisen, Anweisungen oder Anordnungen von zuständigen Aufsichtsbehörden hinsichtlich dieses Annex, werden die Parteien diesen Annex unverzüglich abändern soweit zur Einhaltung solcher geänderten rechtlichen Erfordernisse erforderlich.

19. SCHLUSSBESTIMMUNGEN

19.1 *Vorrang*. Diese Vereinbarung ergänzt die Bedingungen des Vertrags und ist Bestandteil des Vertrags. Im Fall eines Konflikts oder Widerspruchs haben die Bestimmungen dieses Annex Vorrang vor den Bestimmungen des Vertrags. Im Übrigen behalten die Bestimmungen des Vertrags vollumfänglich ihre Gültigkeit.

19.2 *Schriftform*. Änderungen und Ergänzungen dieses Annex und aller ihrer Bedingungen bedürfen zu ihrer Wirksamkeit der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Annex handelt. Dies gilt auch für einen Verzicht auf dieses Formerfordernis.

19.3 *Salvatorische Klausel*. Sollte eine Bestimmung dieses Annex unwirksam oder undurchführbar sein, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die Parteien verpflichten sich, anstelle der unwirksamen oder undurchführbaren Bestimmung eine dieser Bestimmung möglichst wirtschaftlich nahekommende wirksame Regelung zu treffen. Entsprechendes gilt im Fall von lückenhaften Bestimmungen.

SUB-ANNEX 1

Zweck der Verarbeitung, Kategorien der Auftraggeberdaten

und von der Verarbeitung betroffene Personen

Kategorien betroffener Personen	**Kategorien der Auftraggeberdaten**	**Zweck der Datenverarbeitung**
Nutzer und Ansprechpartner	*Identifikationsdaten* *Vor- und Nachname / Titel / / Straße / Hausnummer / Wohnort / Postleitzahl / Land / Telefon / Handy / E-Mail-Adresse* *Individuelle Daten* *Passwörter / Verkehrsdaten Netzwerk / MAC Adresse (wenn personenbeziehbar) / Systemdaten (Konfigurationsinformationen, Update-Informationen, Alarmmeldungen, wenn personenbeziehbar) / IP Konfigurationsinformation, Netzwerkidentifikationsinformationen, wenn personenbeziehbar)*	Verwaltung der Mitarbeiter
Kunden	*Identifikationsdaten* *Vor- und Nachname / Straße / Hausnummer / Wohnort / Postleitzahl / Land / Telefon / Handy / E-Mail Adresse* *Individuelle Daten* *Verkehrsdaten / Telefonverbindungsdaten / Protokolldaten (Log-in / Log-off) / Passwörter / Verkehrsdaten Netzwerk / Systemdaten (Konfigurationsinformationen, Update-Informationen, Alarmmeldungen, wenn personenbeziehbar) / IP Konfigurationsinformation, Netzwerkidentifikationsinformationen, wenn personenbeziehbar*	Nutzerauthentifizierung, Nutzerkommunikation und Verbesserung des Produkts
Sonstige sämtliche Kommunikationspartner	*Identifikationsdaten* *Vor- und Nachname / Telefon / Handy / Fax / E-Mail Adresse* *Individuelle Daten* *Verkehrsdaten / Telefonverbindungsdaten / Protokolldaten (Log-in / Log-off) / IP Konfigurationsinformation, Netzwerkidentifikationsinformationen, wenn personenbeziehbar)*	Kontaktherstellung und Protokollierung

SUB-ANNEX 2

Technische und organisatorische Maßnahmen („TOM“)

Alasco hat die folgenden technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO zur Gewährleistung von Verschlüsselung und Pseudonymisierung, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit, Wiederherstellbarkeit sowie entsprechende Verfahren zur Überprüfung implementiert.

1. **MASSNAHMEN ZUR GEWÄHRLEISTUNG VON DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN**

1.1 Es sind geeignete technische und organisatorische Maßnahmen umzusetzen, welche den Anforderungen an die DS-GVO genügen sowie durch geeignete Voreinstellungen sicherzustellen, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

1.2 Alasco berücksichtigt die Anforderungen des Art. 25 DS-GVO bereits in der Konzeptionierungs- und Entwicklungsphase der Produktentwicklung. Prozesse und Funktionalitäten werden dabei so aufgesetzt, dass die Datenschutzgrundsätze wie Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, etc. sowie die Sicherheit der Verarbeitung frühzeitig berücksichtigt werden.

2. **MASSNAHMEN ZUR SICHERSTELLUNG DER VERTRAULICHKEIT**

2.1 Organisationskontrolle

(a) Organisationsanweisungen

(i) Die Ziele im Datenschutz und in der Informationssicherheit sind in einer Datenschutz- und Informationssicherheits-Richtlinie festgelegt und für alle Mitarbeiter von Alasco verbindlich. Darüber hinaus sind weitere Organisationsanweisungen implementiert, um den Mitarbeitern konkrete Richtlinien im Rahmen der Verarbeitung von personenbezogenen Daten zu vermitteln (bspw. Richtlinie zur Nutzung von IT, Internet und E-Mail).

(b) Verpflichtung auf Vertraulichkeit und Datenschutz

(i) Alle Beschäftigten werden bei Aushändigung ihres Arbeitsvertrages bzw. spätestens zu Beschäftigungsbeginn schriftlich auf Vertraulichkeit und Datenschutz sowie auf sonstige einschlägige Gesetze verpflichtet. Die Verpflichtung gilt über die Beschäftigungsdauer hinaus. Freiberufliche Mitarbeiter oder externe Dienstleister werden schriftlich mit Unterzeichnung des Rahmenvertrags u.a. zur Verschwiegenheit verpflichtet.

(c) Einschränkung der Privat- und betrieblichen Nutzung von Kommunikationsmitteln

(i) Das Internetsystem dürfen nur eingeschränkt privat genutzt werden. Es ist dabei strikt auf eine Trennung von privaten und betrieblichen Daten zu achten. Weiterhin ist es den Mitarbeitern von Alasco nicht gestattet, personenbezogene Daten oder sonstige Daten des Auftraggebers, insbesondere aus dem Auftrag, auf privaten Kommunikationsmitteln zu verarbeiten. Die Mitarbeiter von Alasco verpflichten sich zur Einhaltung entsprechender Richtlinien, deren Einhaltung im Rahmen des zulässigen und notwendigen Umfangs kontrolliert wird.

(d) Personalsicherheit

(i) Alasco setzt Maßnahmen vor, während und nach der Beschäftigung zur Sicherstellung der Personalsicherheit um. Darunter fallen in der Regel:

- Niedergeschriebene Vereinbarungen zur Festlegung von Verantwortlichkeiten
- Durchführung von Sensibilisierungs- sowie Kontrollmaßnahmen
- Durchführung eines dokumentierten Offboarding-Prozesses (inkl. Rücknahme von Schlüsseln/Zutrittskarten, Entziehung von Zugriffsrechten, Sicherstellung der ausreichenden Dokumentation, Herausgabe und Weitergabe von Daten, Informationen und Wissen etc.) bei Beendigung des Arbeitsverhältnisses

2.2 Verschlüsselung und Pseudonymisierung personenbezogener Daten

(a) Schlüsselverwaltung

(i) Zum Gebrauch, zum Schutz und zur Lebensdauer von Schlüsseln sowie zum Einsatz von Verschlüsselungsverfahren nach dem Stand der Technik setzt Alasco eine Richtlinie zur Verwendung von kryptographischen Verfahren um. Demnach erfolgt die Generierung und Verwaltung des Hauptschlüssels („Master Key“) außerhalb der Infrastruktur des von Alasco eingesetzten Infrastructure as a Service-Providers sowie Rechenzentrumsbetreibers. Eine Übertragung der Schlüssel außerhalb der Virtual Private Cloud und die Speicherung innerhalb der genutzten Infrastruktur erfolgt ausschließlich verschlüsselt. Der Zugriff auf die Schlüsselverwaltung wird protokolliert und automatisiert sowie bei konkretem Verdacht durch autorisiertes Personal von Alasco auf Unregelmäßigkeiten überprüft. Die entsprechenden Schlüssel werden in regelmäßigen Abständen rotiert und bisher verwendete Schlüssel unmittelbar invalidiert und entfernt. Zudem werden Schlüssel strikt nach Netzwerken bzw. Datenbanken getrennt (bspw. keine Überführung eines Schlüssels in ein anderes Netzwerk). Im Rahmen einer regelmäßigen Sicherheitsprüfung wird sichergestellt, dass die Maßnahmen zur Schlüsselrotation wirksam sind und alte Schlüssel ordnungsgemäß entfernt wurden.

(b) Datenbank- und Speicher-Verschlüsselung

(i) Auf allen von Alasco eingesetzten Datenbanken wird eine Verschlüsselung „at Rest“ nach dem Stand der Technik eingesetzt, sodass die Daten aus der Datenbank nur nach ordnungsgemäßer Authentifizierung am jeweiligen Datenbank-System gelesen werden können. Die zur Speicherung von Dokumenten eingesetzten Speichermedien („Storage“) werden ebenfalls auf Dateisystemebene verschlüsselt. Backups der Datenbank-Systeme werden ausschließlich verschlüsselt aufbewahrt.

(c) Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen („Data in Transit“)

(i) Alle personenbezogenen Daten, die von der Alasco-Applikation an einen Client oder an andere Plattformen über ein unsicheres oder öffentliches Netzwerk übertragen werden, werden ausschließlich verschlüsselt übertragen. Dies gilt insbesondere auch für Zugriffe auf das Kunden- und Admin-System. Alasco gewährleistet die Verwendung einer Verschlüsselungsmethode nach dem Stand der Technik in Abhängigkeit des auf Auftraggeber-Seite kompatiblen Verschlüsselungsalgorithmus (derzeit HTTPS-Verbindungen bzw. Transport Layer Security (TLS), Stichwort „Abwärtskompatibilität: der Auftraggeber ist dafür verantwortlich, mit dem Stand der Technik kompatible Endgeräte/ Browser einzusetzen). Administrative Zugriffe auf Server-Systeme von Alasco sowie die Übertragung von Backups erfolgen ausschließlich über verschlüsselte Verbindungen, bspw. Secure Shell (SSH)- bzw. Virtual Private Network (VPN). Für den Zugriff auf Kunden-Systeme im Rahmen der Heim- und Telearbeit wird eine VPN-Verbindung verwendet. Dabei werden ausschließlich VPN-Server verwendet, welche unter der unmittelbaren Kontrolle von Alasco stehen. Der Einsatz von öffentlichen VPN-Providern ist nicht zulässig.

2.3 Zutrittskontrolle

(a) Türsicherung

(i) Die Eingangstüren zu den Büroräumen von Alasco sind grundsätzlich verschlossen.

(b) Kontrollierte Schlüsselvergabe

(i) Es erfolgt eine zentrale, dokumentierte Schlüsselvergabe an die Mitarbeiter von Alasco seitens dem Bürogebäudebetreiber/Vermieter.

(c) Beaufsichtigung und Begleitung von Fremdpersonen

(i) Ein Zutritt externer Dienstleister und sonstiger Fremdpersonen darf nur durch vorherige Autorisierung und Begleitung durch einen Mitarbeiter von Alasco erfolgen.

(d) Geschlossene Türen und Fenster

(i) Mitarbeiter sind organisatorisch dazu angewiesen, Fenster und Türen außerhalb der Bürozeiten geschlossen bzw. verschlossen zu halten.

(e) Physische und umgebungsbezogene Sicherheit der Server-Systeme in den Rechenzentren

(i) Alasco setzt ausschließlich Server-Systeme von Rechenzentrumsbetreibern ein, die eine gültige Zertifizierung nach ISO/IEC 27001 besitzen und demnach entsprechende technische und organisatorische Maßnahmen zur physischen und umgebungsbezogenen Sicherheit umsetzen, bspw.:

- Das Rechenzentrum und die dort verwendeten Systeme sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind.
- Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.
- Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.
- Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.
- Zutritt zu sensiblen Bereichen wird zusätzlich durch Videoüberwachung überwacht.
- Ausgebildete Sicherheitskräfte bewachen das Rechenzentrum und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

2.4 Zugangskontrolle

(a) Verwendung von Authentifizierungsverfahren

(i) Authentifizierungsverfahren IT-System/ Laptop

- Authentifizierung mit Benutzername und Passwort

(ii) Authentifizierungsverfahren Kunden-System

- Authentifizierung mit E-Mail-Adresse
- Selbstgewähltes Passwort (8 Zeichen, Zahlen, Buchstaben und Sonderzeichen; Einhaltung technisch erzwungen)

- Zurücksetzen des Passworts via E-Mail Reset-Link

(iii) Authentifizierungsverfahren Server-/ Datenbank-System

- Administrative Zugriffe erfolgen über VPN und/ oder SSH

(b) Verwendung sicherer Passwörter

(i) Bei der Vergabe und regelmäßigen Aktualisierung von sicheren Passwörtern sind die Maßgaben des BSI IT Grundschutz oder anderer äquivalenter, anerkannter Sicherheitsstandards für den Alasco Account sowie für die Laptops, Computer oder sonstige mobile Endgeräte zu berücksichtigen (d.h. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennwortes). Nutzer von Alasco sind dazu angehalten, vergleichbare Maßnahmen zur Sperrung bei Inaktivität treffen. Der Auftraggeber hat dafür Sorge zu tragen.

(c) Verbot der Weitergabe von Passwörtern

(i) Sowohl für Nutzer der Alasco-Software, als auch Mitarbeiter, gilt das Verbot der Weitergabe von Passwörtern.

(d) Automatische Sperrung bei Inaktivität

(i) Laptops der Mitarbeiter von Alasco werden bei Nichtbenutzung vom Benutzer mit Passwortschutz gesperrt. Nutzer von Alasco sind dazu angehalten, vergleichbare Maßnahmen zur Sperrung bei Inaktivität zu treffen. Der entsprechende Auftraggeber hat dafür Sorge zu tragen.

(e) Einsatz von Anti-Viren-Software

(i) Laptops der Mitarbeiter von Alasco sind mit einer dem Stand der Technik entsprechende und aktuell gehaltene Anti-Viren-Software auf allen betrieblichen oder betrieblich genutzten IT-Systemen ausgestattet. Es dürfen grundsätzlich keine Rechner ohne residenten Virenschutz betrieben werden, es sei denn, es sind andere äquivalente Sicherheitsmaßnahmen nach dem Stand der Technik getroffen oder ein Risiko besteht nicht. Vorgegebene Sicherheitseinstellungen dürfen nicht deaktiviert oder umgangen werden.

(f) „Clean Desk Policy“

(i) Mitarbeiter von Alasco sind dazu angehalten, personenbezogene Daten von Kunden nicht auszudrucken oder lokal zu speichern, Arbeitsmaterialien grundsätzlich nicht offen herumliegen zu lassen und ordentlich zu verstauen. Unterlagen mit personenbezogenen Daten sind nach Gebrauch entweder in abschließbaren Schränken oder Schubfächern zu verstauen oder datenschutzgerecht zu entsorgen.

2.5 Zugriffskontrolle

(a) Rollen- und Berechtigungskonzept

(i) Rollen- und Berechtigungskonzept Kunden-System

- Für Auftraggeber kann ein mehrstufiges Rollenkonzept zur Rechtevergabe individuell konfiguriert werden und dabei zwischen Ansichts- und Bearbeitungsrechten je Funktion bzw. Bereich innerhalb von Alasco für individuelle Nutzer unterscheiden.

(ii) Rollen- und Berechtigungskonzept Admin-System

- Der Zugriff auf das Admin-System ist grundsätzlich auf geschulte Mitarbeiter im Bereich Kundenservice und Produktentwicklung beschränkt. Mitarbeiter aus dem Vertriebs- und Finance-Team haben über das Admin-System lediglich Zugriff auf Kunden-Systeme während

der kostenfreien Testphase bzw. auf entsprechende Abrechnungsdaten und können somit keine Kundendaten einsehen.

(iii) Rollen- und Berechtigungskonzept Server-/ Datenbank-System

- Der Zugriff auf das Server-/ Datenbank-System ist grundsätzlich auf eine begrenzte Anzahl geschulter Mitarbeiter im Bereich Produktentwicklung und Infrastruktur beschränkt.

(b) Vergabe von Zugriffsrechten

(i) Die Vergabe von Zugriffsrechten erfolgt bei Alasco grundsätzlich nach dem „Need-to-Know"-Prinzip. Zugänge erhalten demnach ausschließlich Personen, die ihn nachvollziehbar benötigen und solange sie ihn benötigen. Den Bedarf muss die beantragende Person bei der Beantragung schlüssig begründen. Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein. Vorgesetzte sind verpflichtet, im Falle von Aufgabenwechsel von Mitarbeitern eine entsprechende Korrektur von Berechtigungen zu beantragen. Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die Personalabteilung unverzüglich über anstehende Veränderungen, damit die entsprechenden Berechtigungen entzogen werden können. Der Entzug von Berechtigungen hat nach Möglichkeit binnen 24 Stunden nach Ausscheiden eines Mitarbeiters zu erfolgen.

(c) Einsatz einer Paketfilter-Firewall

(i) Die Server von Alasco nutzen Paketfilter-Firewalls, die sicherstellen, dass keine Dienste direkt aus dem Internet erreichbar sind. Öffentlich erreichbare Dienste werden über Loadbalancer oder Bastion-Hosts geleitet, die ausschließlich die Protokolle, die für den jeweiligen Dienst benötigt werden, zulassen.

(d) Protokollierung von An- und Abmeldevorgängen

(i) Anmeldeversuche zum und sowie Abmeldevorgänge von Admin-, Kunden-System und Server-Systemen/ -Software werden protokolliert (min. E-Mail-Adresse, Benutzer ID, IP-Adresse, Ergebnis des Anmeldeversuchs sowie Zeitstempel) und derzeit für bis zu 30 Tage aufbewahrt. Diese Protokolle können auf Anfrage und/ oder bei konkretem Verdacht ausgewertet werden.

2.6 Trennbarkeit

(a) Trennung von Entwicklungs-, Test- und Betriebsumgebungen

(i) Daten aus der Betriebsumgebung dürfen nur in Entwicklungsumgebungen überführt werden, wenn sie vor der Überführung vollständig anonymisiert wurden. Die Übertragung der anonymisierten Daten muss verschlüsselt oder über ein vertrauenswürdiges Netz erfolgen. Software, die in die Betriebsumgebung überführt werden soll, muss zuerst in einer identischen Test-Umgebung („Staging") getestet werden. Programme für Fehleranalysen oder das Erstellen/ Kompilieren von Software dürfen in der Betriebsumgebung nur verwendet werden, wenn sich dies nicht vermeiden lässt. Dies ist vor allem dann der Fall, wenn Fehlersituationen von Daten abhängig sind, die aufgrund der Anforderungen für die Anonymisierung bei der Überführung in Testumgebungen verfälscht würden.

(b) Trennung in Netzwerken

(i) Alasco trennt seine Netzwerke nach Aufgaben. Hierbei kommen die folgenden Netzwerke dauerhaft zum Einsatz: Betriebsumgebung („Production"), Testumgebung („Staging"), Office-IT Mitarbeiter, Office-IT Gäste. Zusätzlich zu diesen Netzwerken werden bei Bedarf weitere separate Netzwerke erstellt, z.B. für Restore-Tests und Penetration-Tests. Die Trennung der Netzwerke erfolgt, je nach technischen Möglichkeiten, physisch oder mittels virtueller Netzwerke.

(c) Softwareseitige Mandantentrennung

(i) Alasco stellt die getrennte Verarbeitung und Speicherung von Daten unterschiedlicher Auftraggeber über eine logische Mandantentrennung auf Basis einer Multi-Tenancy-Architektur sicher. Die Zuordnung und Identifizierung der Daten erfolgt dabei über die Zuweisung einer eindeutigen Kennung je Auftraggeber (bspw. Kundennummer/ „Company ID"). Die Absicherung der Architektur erfolgt durch die Implementierung von Integrationstests, welche sicherstellen, dass keine Datenbank-Abfragen ohne Abfrage und Zuordnung zu dieser Kennung durchgeführt werden und das Risiko der Umgehung der Mandantentrennung durch Programmierfehler minimiert wird. Regelmäßige Security-Audits sowie verbindliche Code-Reviews (4- bis 6-Augen-Prinzip) sichern die Architektur zusätzlich ab.

3. MASSNAHMEN ZUR SICHERSTELLUNG DER INTEGRITÄT

3.1 Transport- und Weitergabekontrolle

(a) Transportverschlüsselung („Data in Transit")

(i) Siehe „Verschlüsselung und Pseudonymisierung personenbezogener Daten", Sicherstellung der Integrität der Daten beim Transport durch das Berechnen von Prüfsummen.

(b) Verbot der Weitergabe an unberechtigte Dritte

(i) Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang der Weisungen und soweit dies zur Erbringung der vertraglichen Leistungen für den Auftraggeber erforderlich ist. Insbesondere ist eine Weitergabe von personenbezogenen aus dem Auftrag an unberechtigte Dritte, bspw. durch Speicherung in einem anderen Cloud-Speicher, nicht zulässig.

(c) Protokollierung der Weitergabe von Daten

(i) Siehe "Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung" unter "2.8. Eingabekontrolle"

3.2 Eingabekontrolle

(a) Protokollierung von Systemaktivitäten innerhalb des Admin- und Kunden-Systems sowie Auswertung

(i) Wesentliche Systemaktivitäten werden protokolliert (min. Benutzer ID, Rechte gemäß Rollenkonzept, IP Adresse, Systemkomponenten oder Ressourcen, Art der durchgeführten Aktivitäten sowie Zeitstempel) und derzeit für bis zu 30 Tage aufbewahrt. Dazu zählen insbesondere die Eingabe, Änderung und Löschung von Daten, Nutzern und Berechtigungen sowie die Änderung von Systemeinstellungen. Auf Anfrage und/ oder bei konkretem Verdacht kann eine entsprechende Auswertung der Protokolle durchgeführt werden.

3.3 Verfügbarkeitskontrolle

(a) Datensicherungsverfahren/ Backups

(i) Alasco setzt zur Gewährleistung einer angemessenen Verfügbarkeit ein Backup-Konzept für die Datenbank mit den darauf gespeicherten Daten des Auftraggebers sowie das Speichermedium mit entsprechenden gespeicherten Dokumenten nach dem Stand der Technik um.

(b) Warnsysteme zur Überwachung der Erreichbarkeit und des Zustandes der Server-Systeme

(i) Es existiert ein Warnsystem zur Überwachung der Erreichbarkeit und des Zustandes der Server-Systeme. Bei Ausfällen wird die Infrastruktur-Abteilung automatisch benachrichtigt, um unmittelbar Maßnahmen zur Problembeseitigung zu ergreifen.

(c) IT-Störungsmanagement („Incident Response Management“)

(i) Es existiert ein Konzept und dokumentierte Verfahren zum Umgang mit Störungen und sicherheitsrelevanten Ereignissen („Incidents“). Dies umfasst insbesondere die Planung und Vorbereitung der Reaktion auf Vorfälle, Verfahren zur Überwachung, Erkennung und Analyse von sicherheitsrelevanten Ereignissen sowie die Festlegung entsprechender Verantwortlichkeiten und Meldewege im Falle einer Verletzung des Schutzes personenbezogener Daten im Rahmen der gesetzlichen Vorgaben.

(d) Weitere Maßnahmen zur Gewährleistung der Verfügbarkeit in den Rechenzentren

(i) Im Rechenzentrum ist eine automatische Branderkennung und -bekämpfung installiert. Das System zur Branderkennung setzt Rauchsensoren in der gesamten Umgebung der Rechenzentren, in mechanischen und elektrischen Bereichen der Infrastruktur, Kühlräumen und sowie in den Räumen, in denen die Generatoren untergebracht sind, ein. Alle Stromversorgungssysteme sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Das Rechenzentrum verfügt darüber hinaus über Generatoren, die die gesamte Anlage mit Notstrom versorgen können. Das Rechenzentrum verfügt über eine Klimatisierung und Temperaturkontrolle. Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

3.4 Wiederherstellbarkeit

(a) Regelmäßige Tests der Datenwiederherstellung („Restore-Tests“)

(i) Es werden regelmäßige vollständige Restore-Tests zur Sicherstellung der Wiederherstellbarkeit im Falle eines Notfalls/ einer Katastrophe durchgeführt.

(b) Notfallplan („Disaster Recovery Concept“)

(i) Es existiert ein Konzept zur Behandlung von Notfällen/ Katastrophen sowie ein entsprechender Notfallplan. Alasco stellt die Wiederherstellung aller Systeme auf Basis der Datensicherungen/ Backups, in der Regel innerhalb von 24 Stunden, sicher.

4. MASSNAHMEN ZUR ÜBERPRÜFUNG UND EVALUIERUNG

4.1 Unabhängige Überprüfung der Informationssicherheit

(a) Überprüfung der Einhaltung von technischen Vorgaben

(i) Zur Überprüfung der Sicherheit der Anwendungen und Infrastruktur sowie der regelmäßigen Weiterentwicklung des Produkts werden regelmäßige automatisierte und manuelle Schwachstellenscans durch den CTO oder anderes qualifiziertes Personal durchgeführt. Bei Bedarf werden detaillierte Penetrationstests durch einen externen Dienstleister durchgeführt, um die Anwendungen und Infrastruktur gezielt auf Schwachstellen zu untersuchen.

(b) Auftragskontrolle

(i) Sorgfältige Lieferantenauswahl

- Die Beauftragung von Lieferanten/ Drittanbietern erfolgt bei Auslagerungen auf Basis eines sorgfältigen Auswahlprozesses in Zusammenarbeit mit dem CTO und der Rechtsabteilung nach festgelegten Kriterien, insbesondere hinsichtlich Datenschutz und IT-Sicherheit, dabei insbesondere auf die Prüfung der Dokumentation und Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO.

(ii) Zur Risikoprävention wird im Rahmen des Prozesses ebenfalls eine Risikobewertung für die jeweiligen Lieferanten durchgeführt, sofern der Drittanbieter regelmäßig mit personenbezogenen Daten arbeitet.

(c) Auftragsverarbeitung gemäß Art. 28 DS-GVO

(i) Eine Beauftragung und Nutzung eines Unterauftragnehmers erfolgt ausschließlich im Einklang des Auftragsverarbeitungsvertrags zwischen Alasco und dem Auftraggeber, gesetzlichen Bestimmungen, sowie nach Abschluss einer entsprechenden Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zwischen Alasco und dem Unterauftragnehmer. Diese Vereinbarung hat nach Möglichkeit regelmäßig mindestens folgende Aspekte zu berücksichtigen:

- Vereinbarung wirksamer Kontrollrechte (im Einklang mit Rechten des Auftraggebers, nach Möglichkeit auch Vor-Ort-Kontrollen)
- Vereinbarung entsprechender Kontroll- und Auskunftsrechte bei der Beauftragung weiterer Unterauftragnehmer
- Vereinbarung von Vertragsstrafen bei Verstößen, sofern notwendig und möglich
- Ausschließliche Verarbeitung auf dokumentierte Weisung
- Ausschluss unzulässiger Verarbeitungsschritte
- Verbot der Anfertigung von Kopien von personenbezogenen Daten (ausgenommen Sicherungskopien/ Backups)
- Verpflichtung der Mitarbeiter des Unterauftragnehmers auf Vertraulichkeit
- Mitwirkung bei der Wahrung der Betroffenenrechte etc.
- Informationspflichten bei meldepflichtigen Verletzungen des Schutzes personenbezogener Daten nach den Art. 33 und 34 DS-GVO, Betriebsstörungen sowie sonstigen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten
- Sicherstellung der Löschung/ Vernichtung von Daten nach Beendigung des Auftrags

(d) Durchführung regelmäßiger Kontrollen/ Einforderung von Nachweisen

(i) Alasco wird sich vor Beginn der Beauftragung und danach regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen der von ihr eingesetzten Unterauftragnehmer überzeugen bzw. diese nachweisen lassen.

SUB-ANNEX 3

Genehmigte Subunternehmer

Subunternehmer	Zweck der Verwendung	Weitere Informationen
Amazon Web Services (‘Amazon.com, Inc.’)	Amazon Web Services ist der Anbieter der Alasco Server-Infrastruktur	https://aws.amazon.com/privacy/
Chargebee, Inc.	Dient der Rechnungsstellung	https://www.chargebee.com/security/#eu-us-privacy-shield
Churnzero, Inc.	Unterstützung des Kunden bei der Implementierung der Software und fortlaufender Support	https://churnzero.net/privacy-policy/
Google Apps (‘Google, Inc.’)	Google Apps Produkte (Gmail, GoogleDrive) dienen zur internen Kommunikation und Ablage von Dokumenten	https://policies.google.com/privacy?hl=de
Google Tag Manager (’Google, Inc.’)	Ein Tool zur Verwaltung von sog. Tags, welche beim Tracking im Online Marketing eingesetzt werden. Der Tag Manager selber verarbeitet dabei keine personenbezogenen Daten, da er rein der Verwaltung von anderen Diensten – bspw. Google Analytics, etc. – dient	https://policies.google.com/privacy?hl=de
Joincube Inc. (‘Beamer’)	Dient zur Information über Produkt-Neuerung, Updates, Live-Demos und neue Blog-Inhalte in der Alasco App.	https://www.getbeamer.com/privacy-policy
Klippa App B.V.	Digitalisierung von Dokumenten	https://www.klippa.com/
OneSignal, Inc.	Das Senden von Push-Nachrichten in unserer Alasco App	https://onesignal.com/privacy_policy
SendGrid, Inc.	Cloud basierter Kommunikationsdienstleister zur Versendung von transaktionalen E-Mails	https://sendgrid.com/solutions/email-api/
Zendesk, Inc.	Bearbeitung von Support-Anfragen im Rahmen der Nutzung der Software sowie Bereitstellung eines Help Centers zur Beantwortung wiederkehrender Anfragen	https://www.zendesk.com/product/zendesk-security/