Vereinbarung zur Auftragsbearbeitung

zwischen

NAME, ADRESSE, VERTRETEN DURCH….

- nachfolgend „Verantwortlicher“ –

und

smino AG, Werkstrasse 20, 8645 Rapperswil-Jona, vertreten durch [EINFÜGEN]

- nachfolgend „Auftragsbearbeiter“ -

- beide nachfolgend gemeinsam „Parteien“ -

wird die folgende Vereinbarung zur Auftragsbearbeitung inklusive aller Anlangen geschlossen:

Präambel

Der Auftragsbearbeiter erbringt für den Verantwortlichen Leistungen im Bereich [IN WELCHEM BEREICH EINFÜGEN] gemäss Vertrag vom XX.XX.XXXX (im Folgenden «Hauptvertrag»). Teil der Durchführung des Hauptvertrages ist die Bearbeitung von personenbezogenen Daten im Sinne der anwendbaren Datenschutzgesetze. Zur Erfüllung der Anforderungen schliessen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

1. Gegenstand der Beauftragung / Umfang der Beauftragung

(1) Die Zusammenarbeit der Parteien nach Massgabe des Hauptvertrages bringt es mit sich, dass der Auftragsbearbeiter Zugriff auf personenbezogene Daten des Verantwortlichen (nachfolgend „Verantwortlichendaten“) erhält und diese ausschliesslich im Auftrag und nach Weisung des Verantwortlichen i.S.d. Art. 4 Nr. 8 und Art. 28 DSGVO bearbeitet.

(2) Die Bearbeitung der Verantwortlichendaten durch den Auftragsbearbeiter erfolgt ausschliesslich in der in Anlage 1 spezifizierten Art sowie in dem dort spezifizierten Umfang und Zweck. Der Kreis der von der Datenbearbeitung betroffenen Personen ist in Anlage 1 zu diesem Vertrag dargestellt. Die Dauer der Bearbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Dem Auftragsbearbeiter ist eine abweichende oder über die Festlegungen in Anlagen 1 hinausgehende Bearbeitung von Verantwortlichdaten untersagt.

(4) Die Bearbeitung der Verantwortlichendaten findet ausschliesslich im Gebiet der Schweiz, in einem Mitgliedstaat der EU oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 bis Art. 49 DSGVO erfüllt sind.

(5) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragsbearbeiter und seine Beschäftigten oder durch den Auftragsbearbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

2. Weisungsbefugnisse des Verantwortlichen

(1) Der Auftragsbearbeiter bearbeitet die Verantwortlichendaten nur im Rahmen der Beauftragung und ausschliesslich im Auftrag und nach Weisung des Verantwortlichen i.S.v. Art. 28 DSGVO (Auftragsbearbeitung), dies gilt insbesondere in Bezug auf Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Verantwortliche hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Bearbeitungstätigkeiten zu erteilen (nachfolgend „Weisungsrecht“). Wird der Auftragsbearbeiter durch andere hoheitliche Akte, denen er unterliegt, zu weiteren Bearbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Bearbeitung mit.

(2) Weisungen werden vom Verantwortlichen grundsätzlich schriftlich erteilt; mündlich erteilte Weisungen sind vom Auftragsbearbeiter schriftlich zu bestätigen. Bei einem Wechsel oder einer längerfristigen Verhinderung der bezeichneten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter schriftlich zu nennen. Der Auftragsbearbeiter wird dem Verantwortlichen einen Wechsel der Person des Weisungsberechtigten frühzeitig anzeigen. Bis zum Zugang einer solchen Mitteilung beim Verantwortlichen gelten die bezeichneten Personen weiter als empfangsberechtigt.

(3) Ist der Auftragsbearbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstösst, hat er den Verantwortlichen darauf hinzuweisen. Der Auftragsbearbeiter ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird.

3. Schutzmassnahmen des Auftragsbearbeiters

(1) Der Auftragsbearbeiter beachtet die gesetzlichen Bestimmungen über den Datenschutz und wird die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weitergeben oder deren Zugriff aussetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragsbearbeiter alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrags betraut werden (im folgenden „Mitarbeiter“), in Schriftform zur Vertraulichkeit gemäss Art. 28 Abs. 3 lit b. DSGVO verpflichten und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen.

(3) Der Auftragsbearbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Massnahmen (nachfolgend „TOMs“) zum angemessenen Schutz der Verantwortlichendaten gemäss Art. 32 DSGVO, insbesondere die in Anlage 2 zu diesem Vertrag aufgeführten Massnahmen, zu ergreifen und diese für die Dauer der Bearbeitung der Verantwortlichendaten aufrechtzuerhalten.

(4) Eine Änderung der getroffenen TOMs bleibt dem Auftragsbearbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

4. Informations- und Unterstützungspflichten des Auftragsbearbeiters

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsbearbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmässigkeiten bei der Bearbeitung der Verantwortlichendaten durch den Auftragsbearbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsbearbeiter den Verantwortlichen unverzüglich, spätestens innerhalb von 72 Stunden in elektronischer Form informieren. Dasselbe gilt für Prüfungen des Auftragsbearbeiters durch die Datenschutz-Aufsichtsbehörde. Die Meldungen gemäß Ziffer 4 Abs. 1 S. 1 enthalten jeweils zumindest die in Art. 33 Abs. 3 DSGVO genannten Angaben. Das Template in Anhang 3 ist hierfür zu nutzen. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

(2) Der Auftragsbearbeiter wird den Verantwortlichen im Falle der Ziffer 4 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmassnahmen im Rahmen des Zumutbaren unterstützen. Der Auftragsbearbeiter wird insbesondere die erforderlichen Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Verantwortlichen hierüber informieren und diesen um weitere Weisungen ersuchen.

(3) Der Auftragsbearbeiter verpflichtet sich, dem Verantwortlichen auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle gemäss Ziffer 7 Abs. 1 dieses Vertrages erforderlich sind.

5. Sonstige Verpflichtungen des Auftragsbearbeiters

(1) Der Auftragsbearbeiter ist verpflichtet ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Bearbeitung gemäss Art. 30 Abs. 2 DSGVO zu führen.

(2) Sollten die Verantwortlichendaten beim Auftragsbearbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat der Auftragsbearbeiter den Verantwortlichen darüber zu informieren. Der Auftragsbearbeiter wird in diesem Zusammenhang alle zuständigen Stellen darüber informieren, dass die Entscheidungshoheit über die Daten ausschliesslich beim Verantwortlichen liegt.

6. Subunternehmerverhältnisse

(1) Der Auftragsbearbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von Unterauftragsverhältnissen mit Subunternehmern ("Subunternehmerverhältnis") befugt. Beauftragt der Auftragsbearbeiter Subunternehmer, so hat er dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den von ihm beauftragten Subunternehmen gelten, wobei dem Verantwortlichen gegenüber dem Subunternehmer sämtliche Kontrollrechte gemäss Ziffer 7 dieses Vertrages einzuräumen sind. Der Auftragsbearbeiter darf weitere Unter-Auftragsbearbeiter („Subunternehmen“) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen i.S.v. Art. 28 Abs. 2 DSGVO. Sofern es sich um eine allgemeine schriftliche Genehmigung Im Sinne von Satz 1 handelt, informiert der Auftragsbearbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann innerhalb von zwei Wochen gegen derartige Änderungen Einspruch erheben. Subunternehmerverhältnisse zu Dritten ausserhalb der Schweiz oder des Europäischen Wirtschaftsraumes sind nicht gestattet, außer eine schriftliche oder elektronische Zustimmung seitens des Verantwortlichen liegt vor.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsbearbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen

sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsbearbeiter für den Verantwortlichen erbringt sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenbearbeitungsanlagen. Die Pflicht des Auftragsbearbeiters, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

7. Kontrollrechte

(1) Der Verantwortliche ist berechtigt, sich regelmässig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der TOMs gemäss Ziffer 3 Abs. 3 dieser Vereinbarung, zu überzeugen i.S.v. Art. 28 Abs. 3 S. 2 lit. h DSGVO. Hierfür kann er z.B. Auskünfte des Auftragsbearbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die TOMs des Auftragsbearbeiters dort zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsbearbeiter steht und die persönliche Kontrolle angekündigt wird.

(2) Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragsbearbeiters nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig, mindestens jedoch 4 (vier) Wochen im Voraus. Diese Beschränkungen gelten nicht, soweit eine Verletzung des Schutzes personenbezogener Daten beim Auftragsbearbeiter offensichtlich zugrunde liegt.

(3) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsbearbeiter mit. Bei Fehlern oder Unregelmässigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsbearbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsbearbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

8. Rechte Betroffener

(1) Der Auftragsbearbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten TOMs bei der Erfüllung von dessen Pflichten. Er wird dem Verantwortlichen innerhalb von 6 (sechs) Werktagen, die gewünschte Auskunft über Verantwortlichendaten geben, sofern der Verantwortliche nicht selbst über die entsprechenden Informationen verfügt.

(2) Macht der Betroffene Rechte seine Rechte gemäss Art. 16 bis 18 DSGVO geltend, ist der Auftragsbearbeiter dazu verpflichtet, die Verantwortlichendaten auf Weisung des Verantwortlichen binnen einer Frist von 6 (sechs) Werktagen zu berichtigen, löschen oder deren Bearbeitung einzuschränken. Der Auftragsbearbeiter wird dem Verantwortlichen die Löschung, Berichtigung bzw. Einschränkung der Bearbeitung der Daten auf Verlangen schriftlich nachweisen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsbearbeiter geltend, wird der Auftragsbearbeiter dieses Ersuchen an den Verantwortlichen weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragsbearbeiter nicht mit der betroffenen Person in Kontakt treten.

9. Laufzeit und Kündigung

(1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

(2) Der Verantwortliche ist jederzeit zu einer ausserordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragsbearbeiter seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der einschlägigen Datenschutzbestimmungen vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Verantwortlichen nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstössen setzt der Verantwortliche dem Auftragsbearbeiter zunächst eine angemessene Frist, innerhalb welcher der Auftragsbearbeiter den Verstoss abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Verantwortlichen sodann das Recht zur ausserordentlichen Kündigung zu.

10. Löschung und Rückgabe nach Vertragsende

(1) Der Auftragsbearbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Verantwortlichen, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Verantwortlichendaten beim Auftragsbearbeiter, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemässen Bearbeitung der Verantwortlichendaten dienen. Solche Dokumentationen sind vom Auftragsbearbeiter für eine Dauer von 10 Jahren aufzubewahren und auf Verlangen an dem Verantwortlichen herauszugeben.

(2) Der Auftragsbearbeiter wird dem Verantwortlichen die Löschung schriftlich bestätigen. Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragsbearbeiter in geeigneter Weise zu kontrollieren; Ziffer 7 Abs. 2 dieses Vertrags gilt hierfür entsprechend.

(3) Der Auftragsbearbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln

11. Haftung

(1) Im Falle eines Verstosses gegen Pflichten aus diesem Vertrag kann der Verantwortliche nach eigenem Ermessen entweder verlangen, dass der Auftragsbearbeiter bis zur Behebung des Verstosses unentgeltlich Abhilfe schafft oder den Verstoss durch einen Dritten beheben lässt und alle damit im Zusammenhang entstehenden Kosten vom Auftragsbearbeiter zurückfordern und den Auftragsbearbeiter für sein Verschulden haftbar machen kann, es sei denn, der Auftragsbearbeiter weist nach, dass er keine Vertragspflicht verletzt hat. Gesetzliche Gewährleistungsrechte sowie das Recht, den Auftragsbearbeiter haftbar zu machen oder nach diesem Vertrag zu kündigen, bleiben hiervon unberührt.

(3) Jede Partei haftet gegenüber der anderen für sich und Ihre Vertreter in der Höhe einer Jahresentschädigung bzw. der vereinbarten Vertragssumme für die Verletzung der Gesetze und Vorschriften zum Datenschutz sowie für die Verletzung dieses Vertrages oder einer Datenschutzbestimmung eines Dienstleistungsvertrages, es sei denn, die jeweils andere Partei hat die Verletzung vorsätzlich oder grobfahrlässig verschuldet. Dies ist unter anderem der Fall, wenn der Auftragsbearbeiter auf Anweisung des Verantwortlichen trotz dessen Information über die nicht Gesetzes und Vorschriftenkonforme Unterlassung oder Handlung beauftragt wurde diese trotzdem vorzunehmen.

(4) Jede Partei stellt die andere Partei auf erstes Anfordern von und gegen alle Ansprüche Dritter (einschliesslich der betroffenen Personen) bezüglich eines Verstosses gegen diesen Vertrag, die Gesetze und Vorschriften zum Datenschutz oder gegen datenschutzrelevante Bestimmungen eines Vertrages frei, unabhängig davon, ob dieser Verstoss von der entschädigenden Partei oder einem ihrer Vertreter begangen wurde, sofern der Verstoss von der entschädigenden Partei rechtlich zu vertreten ist. Die Freistellungsverpflichtung der freistellenden Partei umfasst uneingeschränkt alle Schadensersatzansprüche Dritter, einschliesslich der Kosten und Aufwendungen, die der

empfangenden Partei im Zusammenhang mit der Verletzung oder der Abwehr von Ansprüchen Dritter entstehen.

(5) Im Übrigen regelt sich die Haftung, sofern die DSGVO Anwendung findet, der Parteien nach Art. 82 DSGVO. Eine Haftung des Auftragsbearbeiter gegenüber dem Verantwortlichen wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

12. Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass dem Auftragsbearbeiter ein Zurückbehaltungsrecht an den Verantwortlichendaten nicht zusteht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt Schweizer Recht. Ausschliesslicher Gerichtsstand ist Rapperswil-Jona.

Für den Verantwortlichen:

---	---
Ort, Datum	[Name und Funktion]

Für den Auftragsbearbeiter:

---	---
Ort, Datum	[Name und Funktion]

Anlage 1: Gegenstand der Datenbearbeitung
Anlage 2: TOMs
Anlage 3: Template im Fall von Datenschutzverletzungen

Anlage 1: Gegenstand der Datenbearbeitung

Auftragsbearbeitungsvertrag zum Hauptvertrag zwischen smino AG, Werkstrasse 20, 8645 Rapperswil-Jona [«AUFTRAGSBEARBEITER»] und dem VERANTWORTLICHEN.

1. Gegenstand der Datenbearbeitung /Bearbeitungstätigkeit

[Was wird bearbeitet z.B. Speicherung und Bearbeitung von Kundendaten]

2. Zweck der Datenbearbeitung

[WARUM WERDEN DIESE DATEN BEARBEITET z.B. Zur Ermöglichung der Kollaboration zwischen Kunden und Lieferanten]

3. Ort der Bearbeitung der Personendaten

[WO WERDEN DIE DATEN BEARBEITET, in der EU, Schweiz, USA?]

4. Relevante Weitergabe

[SCCs und ADVs mit Dritten geschlossen? Auslandsbezüge?]

5. Genehmigte Sub- bzw. Subsubunternehmer

	Name	Adresse	Kontaktperson	Kontaktdetails	Ort der Datenbearbeitung	Kategorie der bearbeiteten Daten
1.	Dropbox	ergänzen	ergänzen	ergänzen	ergänzen	ergänzen
2.						

6. Personendatenkategorien [Wenn möglich Kategorien gem. Verfahrensverzeichnis verwenden.]

[PERSONENKATEGORIEN SIND Z.B: KUNDENDATEN, LIEFERANTEN, PERSONAL]

7. Besondere Kategorien von Personendaten [Wenn möglich Kategorien gem. Verfahrensverzeichnis verwenden.

[DENKE NICHT]

8. Kategorien von betroffenen Personen [Wenn möglich Kategorien gem. Verfahrensverzeichnis verwenden.]

[Welche Personen – Kunden, Lieferanten?]

Anlage 2: Technisch-organisatorische Massnahmen

Auftragsbearbeitungsvertrag zum Hauptvertrag zwischen smino AG, Werkstrasse 20, 8645 Rapperswil-Jona [«AUFTRAGSBEARBEITER»] und dem VERANTWORTLICHEN.

1. Präambel

(i) Diese technischen und organisatorischen Massnahmen sind auf personenbezogene Daten und Vertrauliche Informationen des Verantwortlichen anwendbar.

2. Organisation

(ii) Der Auftragsbearbeiter besitzt eine dokumentierte und aktuelle Informationssicherheitspolitik (ISP), die er aufrechterhält, umgesetzt und seinen Vertretern kommuniziert hat. Die ISP des Auftragsbearbeiters ist ISO/IEC 27001/27002:2013 angelehnt. Der Auftragsbearbeiter wird dem Verantwortlichen seine ISP und jegliche Ergänzungen auf Aufforderung zur Verfügung stellen.

(iii) Der Auftragsbearbeiter ist verpflichtet, die konkreten Anforderungen der geltenden Gesetze und Vorschriften zum Datenschutz einzuhalten. Dies kann Massnahmen für Folgendes umfassen: Ernennung von Datenschutzbeauftragten; Verpflichtung der Mitarbeiter zur Wahrung der Vertraulichkeit; Schulung von Personal zum Datenschutz und zur Datensicherheit wird umgesetzt; Realisierung von IT-Sicherheitskonzepten; Benachrichtigungen / Genehmigungen im Zusammenhang mit Datenschutzbehörden, sofern zutreffend).

(iv) Um eine versehentliche Vermengung von Daten des Verantwortlichen zu vermeiden, wird der Auftragsbearbeiter insbesondere aus wirtschaftlicher Sicht angemessene Sicherheitsmassnahmen umsetzen, um andere personenbezogene Daten als die, die zum Verantwortlichen gehören (personenbezogener Daten des Verantwortlichen), anhand geeigneter technischer und organisatorischer Massnahmen von der Infrastruktur des Auftragsbearbeiters zu trennen (Beispiele für Massnahmen: physische oder logische Trennung von personenbezogenen Daten).

(v) Der Auftragsbearbeiter wird veranlassen, dass all seine Vertreter, die Zugang zu personenbezogenen Daten und/oder zur Infrastruktur des Verantwortlichen haben, seine Richtlinien und Verfahren, insbesondere dieser Anlage 2, oder jegliche ergänzenden IT-Sicherheitsmassnahmen, die dem Auftragsbearbeiter durch den Verantwortlichen mitgeteilt wurden, einzuhalten. Der Auftragsbearbeiter muss alle angemessenen Vorkehrungen unternehmen, um eine Beschädigung jeglicher Computerausrüstungen, Systeme, Daten und insbesondere personenbezogener Daten des Verantwortlichen oder eines Konzernmitgliedes des Verantwortlichen aufgrund von Handlungen, Unterlassungen oder Fahrlässigkeit seitens des Auftragsbearbeiters oder irgendwelcher seiner Vertreter zu vermeiden.

3. Risikobewertungen

(i) Der Auftragsbearbeiter führt regelmässig (mindestens jährlich) Risikobewertungen durch, um i) angemessenerweise absehbare Bedrohungen zu bestimmen, die einen unbefugten Zugang zu irgendwelchen Daten zur Folge haben könnten oder dazu führen könnten, dass irgendwelche der Daten unbefugt vervielfältigt, genutzt, bearbeitet, offengelegt, verändert, weitergegeben oder vernichtet werden oder verloren gehen, ii) die Wahrscheinlichkeit des Eintritts dieser Bedrohungen und des dadurch unter Umständen verursachten Schadens zu bewerten und iii) zu bewerten, ob die vorhandenen technischen, administrativen und organisatorischen Sicherheitsmassnahmen ausreichend sind, um die Gesetze und Vorschriften zum Datenschutz einzuhalten.

4. Sicherheitsmassnahmen

(i) Sicherheitsmassnahmen müssen dem Stand der Technik, den Kosten für die Implementierung sowie der Art, dem Umfang, dem Zusammenhang und den Zwecken der Bearbeitung sowie der Gefahr für die Rechte und Freiheiten natürlicher Personen Rechnung tragen. Die

angemessenen Sicherheitsmassnahmen des Auftragsbearbeiters müssen einen in Anbetracht des Risikos angemessenen Grad der Sicherheit gewährleisten, soweit angebracht, einschliesslich des Folgenden:

a. Pseudonymisierung oder Verschlüsselung – auf Datenbankebene - der personenbezogenen Daten des Verantwortlichen der Daten die nicht aktiv genutzt werden (Data at Rest);
b. die Fähigkeit, die Aufrechterhaltung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Bearbeitungssysteme und Dienstleistungen sicherzustellen;
c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten des Verantwortlichen und den Zugang zu ihnen nach Eintritt eines physischen oder technischen Vorfalls umgehend wiederherzustellen;
d. ein Verfahren zur regelmässigen Prüfung, Bewertung und Evaluierung der Effizienz technischer und organisatorischer Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung.

(ii) Bei der Bewertung des angemessenen Schutzniveaus sind vor allem die mit der Bearbeitung einhergehenden Risiken zu berücksichtigen, insbesondere infolgedessen, dass weitergegebene, gespeicherte oder anderweitig bearbeitete personenbezogene Daten versehentlich oder unrechtmässig vernichtet werden, verloren gehen, verändert werden oder unbefugt offengelegt oder Zugang verschafft worden ist.

(iii) Die Sicherheitsmassnahmen müssen denjenigen Sicherheitsmassnahmen entsprechen, die gegebenenfalls durch die für den Verantwortlichen geltenden nationalen Gesetze und Vorschriften zum Datenschutz als Mindestanforderung vorgegeben werden.

5. Zugangskontrolle

(i) Der Zugang zu den Einrichtungen, Systemen, Anwendungen und Netzwerken, die für diese Dienstleistungen genutzt werden, wird nur nach dem Prinzip der geringsten Privilegien gewährt.

(ii) Der Auftragsbearbeiter wird sich bemühen, sicherzustellen, dass die personenbezogenen Daten des Verantwortlichen innerhalb der Infrastruktur des Auftragsbearbeiters in einem physisch sicheren Umfeld verwahrt werden, zu dem ausschliesslich befugtes Personal des Auftragsbearbeiters Zugang hat, und dass physische angemessene Sicherheitsvorkehrungen für Medien implementiert werden, um zu verhindern, dass irgendwelche Medien, die personenbezogene Daten des Verantwortlichen enthalten, unbefugt eingesehen, kopiert, verändert oder gelöscht werden.

(iii) Das Prinzip der Aufgabentrennung ist anzuwenden und zu dokumentieren.

(iv) Der Zugang (einschliesslich des physischen Zugangs) zu Systemen, Anwendungen und Netzwerken für den Zugang zu personenbezogenen Daten und Assets, Medien und Datenträgern ist zu protokollieren, und der Zugang zu den Logdateien ist auf befugtes Personal zu beschränken. Der Verantwortliche erhält auf Anforderung Zugang zu einer Kopie der betreffenden Logdateien.

(v) Logdateien sind im Einklang mit den Anweisungen des Verantwortlichen für einen Zeitraum von mindestens sechs (6) Monaten zu verwahren.

(vi) Der Zugang (einschliesslich eines privilegierten Zugangs) zu Systemen für den Zugang zu personenbezogenen Daten und Assets, Medien und Datenträgern ist routinemässig zu überprüfen und - sofern er nicht länger gerechtfertigt ist - unverzüglich zu widerrufen. Personen, die berechtigt sind, ein Datenbearbeitungssystem zu nutzen, erhalten nur dann Zugang zu den personenbezogenen Daten des Verantwortlichen, wenn sie die betreffenden Daten kennen müssen. Darüber hinaus dürfen keine personenbezogene Daten des Verantwortlichen ohne entsprechende Genehmigung während der Bearbeitung oder Nutzung sowie nach der Verwahrung gelesen, kopiert, verändert oder gelöscht werden (Beispiele für Massnahmen: Beschränkung des Zugangs zu Dateien und Programmen auf diejenigen Personen, die sie kennen müssen; Verhinderung der Nutzung/Installation nicht genehmigter Hardware und/oder

Software; Aufbewahrung von Datenträgern in gesicherten Bereichen mittels eines IT-Nutzungsreglements; Festlegung von Regeln für die sichere und dauerhafte Vernichtung von Datenträgern, die nicht länger benötigt werden).

6. Integritätskontrollen

(i) Soweit dies nicht im Hinblick auf die Erbringung der Dienstleistungen im Einklang mit der Vereinbarung notwendig ist, dürfen keine personenbezogenen Daten des Verantwortlichen ohne Genehmigung während der Weitergabe oder Speicherung gelesen, kopiert, verändert oder gelöscht werden, und es muss möglich sein, zu bestimmen, an wen personenbezogene Daten des Verantwortlichen weitergegeben wurden.

(ii) Es muss möglich sein, im Nachhinein zu prüfen und zu bestimmen, ob und durch wen personenbezogene Daten des Verantwortlichen in Datenbearbeitungssysteme eingegeben, aufgerufen, geändert, kopiert oder gelöscht wurden (Beispiele für Massnahmen: Protokollierung der Aktivitäten von Administratoren und Benutzern).

(iii) Personenbezogene Daten des Verantwortlichen, die durch einen Auftragsbearbeiter bearbeitet werden, dürfen nur im Einklang mit der Vereinbarung und den diesbezüglichen Anweisungen des Verantwortlichen bearbeitet werden (Beispiele für Massnahmen können Folgendes umfassen: schriftliche Anweisungen oder Verträge; Kontrolle der Vertragserfüllung).

(iv) Passwort-Management

a. Für alle Systeme und Anwendungen werden starke Passwörter genutzt (mindestens 8 Zeichen, Sonderzeichen, Zahlen und Buchstaben). Die betreffenden Passwörter sind durch den Benutzer bei ihrem erstmaligen Gebrauch und im Anschluss regelmässig zu ändern.
b. Die maximale Anzahl der fehlgeschlagenen aufeinanderfolgenden Anmeldeversuche ist zu begrenzen und im Falle einer Überschreitung ist der Zugang so lange zu sperren, bis das Passwort durch befugtes Personal zurückgesetzt wird.
c. Passwörter werden auf sichere Weise und erst nach Überprüfung der Identität des Antragstellers ausgegeben und zugestellt.
d. Standardpasswörter sind bei ihrem erstmaligen Gebrauch zu ändern.
e. Passwörter dürfen nicht in lesbarer Form gespeichert oder weitergeleitet werden.

7. Verfügbarkeit

(i) Es müssen angemessene Sicherheitsmassnahmen konzipiert werden, um einen Verlust von personenbezogenen Daten des Verantwortlichen infolge einer versehentlichen Zerstörung oder eines anderweitigen Verlusts zu vermeiden (Beispiele für Massnahmen können Folgendes umfassen: Erstellung von Sicherungskopien, die in speziell geschützten Umgebungen verwahrt werden, oder der Aufbau zuverlässiger Redundanzen; Installation von Antivirensoftware; Erstellung von Notfallplänen oder Strategien zur Wiederaufnahme des Geschäftsbetriebs bei Wasserschäden, Blitzschlag, Stromausfällen oder sonstigen Ausfällen seitens des Auftragsbearbeiter).

(ii) Host-Betriebssysteme: Alle Host-Betriebssysteme sind gesichert, was unter anderem Folgendes einschliesst:

a. Zeitlimits für Inaktivität
b. Deaktivierung ungenutzter Ports/Dienste
c. Systeme werden gepatcht und verwenden aktuelle und unterstützte Softwareversionen
d. Viren sind jegliche Viren, Würmer, Trojaner, Malware und andere bösartige Codes oder Fehlfunktionssoftware, Codes oder Tools, Softwareschlösser, Backdoors, Zeitbomben, Programmzugriffsverweigerungen, ähnliche Deaktivierungscodes oder andere Abschaltmechanismen sowie alle sonstigen Funktionen oder Geräte, die in irgendeiner Weise die Nutzung oder den Betrieb der Software oder der personenbezogenen Daten, die dem Verantwortlichen zur Verfügung gestellt oder in die Assets, Medien und Datenträgern des Verantwortlichen oder eines Konzernmitgliedes des Verantwortlichen eingebracht werden, beeinträchtigen oder behindern würden (nachfolgend “Viren” genannt). Anti-Virus-

Lösungen, einschliesslich des zeitnahen Einsatzes aktueller Signaturen: Software oder personenbezogenen Daten, die durch den Auftragsbearbeiter bereitgestellt oder in das System des Verantwortlichen oder eines Konzernmitgliedes des Verantwortlichen eingebracht werden, sind durch den Verantwortlichen vor der Verwendung auf eigene Kosten auf Viren zu überprüfen. Alle Virenprüfungen durch den Verantwortlichen sind vor der Nutzung unter Einsatz einer dem neuesten Stand der Technik entsprechenden (der Softwarebranche zum betreffenden Zeitpunkt zur Verfügung stehenden) Antivirensoftware am Arbeitsstandort des Verantwortlichen durchzuführen. Der Auftragsbearbeiter muss im Einklang mit seinen eigenen Richtlinien und Verfahren Virenprüfungen bei seinen eigenen Systemen durchführen und gegenüber dem Verantwortlichen auf angemessene Aufforderung nachweisen, dass dies erfolgt ist.

8. Schwachstellenprüfungen

(i) Server, Endpunkte, Netzwerke und Anwendungen sind regelmässig zu überprüfen.

(ii) Schwachstellen sind unter Berücksichtigung der mit ihnen einhergehenden Risiken und Konsequenzen abzustellen.

(iii) Der Auftragsbearbeiter verfügt über ein formelles Programm zum Schwachstellen-Management, das auf die Behebung jeglicher Schwachstellen ausgerichtet ist.

9. Netzwerksicherheit

(i) Für den Umgang mit personenbezogenen Daten und die Verbindung zu genutzten Hosts/Infrastruktur, Assets, Medien und Datenträger sind mittels Firewall(s) zu schützen. Die Firewall-Regeln sind auf regelmässiger Grundlage zu prüfen und zu dokumentieren.

(ii) Im Zusammenhang mit der Bearbeitung von personenbezogenen Daten und der Verbindung zu Assets, Medien und Datenträger erfolgt eine netzwerkbasierte Sicherheitsüberwachung.

(iii) Im Zusammenhang mit der Bearbeitung von Personenbezogener Daten und der Verbindung zu Assets, Medien und Datenträger sind Intrusion-Prevention-Systeme implementiert.

(iv) Der Fernzugang zu den Netzwerken des Auftragbearbeiters ist mittels Multi-Faktor-Authentifizierung geschützt, und die Verbindung ist über VPN gesichert.

10. Endbenutzer-Computing

(i) An den für den Zugang zu personenbezogenen Daten oder Assets, Medien und Datenträger des Verantwortlichen genutzten Endpunkten ist eine Antiviren- und Anti-Malware-Software installiert und aktiv, und Signaturupdates werden zeitnah installiert.

(ii) Laptops sind verschlüsselt.

(iii) Kritische Betriebssystem-Patches werden zeitnah installiert.

11. Speicherung von personenbezogenen Daten

(i) Personenbezogene Daten des Verantwortlichen dürfen nicht auf privaten Mobilgeräten oder privaten tragbaren Speichermedien gespeichert werden (einschliesslich von USB-Laufwerken, DVDs, CDs oder tragbaren Festplatten).

(ii) Personenbezogene Daten des Verantwortlichen dürfen auf durch den Auftragsbearbeiter genehmigten Geräten oder tragbaren Speichermedien gespeichert werden, solange sie in einem verschlüsselten Format vorliegen, das auf einer starken Verschlüsselung beruht.

(iii) Sensible personenbezogene Daten, Assets, Medien und Datenträger des Verantwortlichen, die als ‘Eingeschränkt’ eingestuft werden, einschliesslich PII, PHI und PFI, sind bei einer Speicherung im Ruhezustand unter Verwendung einer starken Verschlüsselung zu verschlüsseln.

12. Vernichtung von personenbezogenen Daten, Assets, Medien und Datenträgern des Verantwortlichen

(i) Der Auftragsbearbeiter hat nicht das Recht, personenbezogene Daten, Assets, Medien und Datenträgern des Verantwortlichen ohne vorherige Genehmigung des Verantwortlichen und/oder eines Konzernmitgliedes des Verantwortlichen, die schriftlich oder per E-Mail zu erteilen ist, zu vernichten oder zu vervielfältigen. Der Auftragsbearbeiter wird personenbezogene Daten, Assets, Medien und Datenträgern des Verantwortlichen - sofern sie nicht gesetzlich zu ihrer Verwahrung verpflichtet sind - auf erste Aufforderung des Verantwortlichen und/oder Konzernmitglieder des Verantwortlichen umgehend und vollständig zurückgeben. Dasselbe gilt für den Fall, dass der Auftragsbearbeiter irgendwelche personenbezogenen Daten, Assets, Medien und Datenträger des Verantwortlichen nicht länger benötigt. Der Auftragsbearbeiter wird dem Verantwortlichen und/oder Konzernmitglieder des Verantwortlichen das betreffende Eigentum des Verantwortlichen zurückgeben oder dasselbe vernichten.

(ii) Der Auftragsbearbeiter muss angemessene Sicherheitsvorkehrungen und Verfahren implementieren und aufrechterhalten, um personenbezogene Daten des Verantwortlichen von Computern, Servern, Faxgeräten, Druckern, Kopiergeräten, Scannern, Papierdokumenten und Mobilgeräten usw., die nicht länger genutzt werden, zu entfernen oder zu vernichten.

13. Dokumentation, Prüfung und Untersuchung

(i) Es sind vereinfachte Protokolle zu führen und auf Anfrage herauszugeben, um sicherzustellen, dass die tatsächlich ausgeführten Bearbeitungsschritte, insbesondere Änderungen, Abrufe und Weiterleitungen, im erforderlichen Umfang zurückverfolgt werden können, damit ihre Zulässigkeit überprüft werden kann.

(ii) Die ergriffenen Massnahmen in den Absätzen 1 bis 12 sind zu dokumentieren, um die Kontrolle zu erleichtern und die Aufbewahrung von Beweismitteln sicherzustellen.

(iii) Der Auftragsbearbeiter ist verpflichtet, dem Verantwortlichen auf Anfrage eine Kopie aller Berichte zu Betriebsprüfungen zuzustellen, die durch unabhängige Instanzen durchgeführt wurden.

(iv) Unbeschadet jeglicher Klauseln der Vereinbarung, die das Prüfungs- und Kontrollrecht zum Gegenstand haben, hat der Verantwortliche (zusammen mit seinen externen Prüfern oder beliebigen Aufsichtsbehörden) das Recht, in Abstimmung mit dem Auftragsbearbeiter und unter Einhaltung einer angemessenen Ankündigungsfrist jegliche Aspekte der Sicherheitsmassnahmen und Verfahren des Auftragsbearbeiters zu überprüfen und seine eigenen Sicherheitsprüfungen im Zusammenhang mit den personenbezogenen Daten des Verantwortlichen (einschliesslich von Eindringprüfungen) durchzuführen.

(v) Der Auftragsbearbeiter ist verpflichtet, bei allen derartigen Überprüfungen und Kontrollen umfassend zu kooperieren und Auskünfte ohne unangemessene Verzögerung bereitzustellen. Darüber hinaus ist der Auftragsbearbeiter verpflichtet, den Verantwortlichen ohne unangemessene Verzögerung über jegliche Vorfälle im Zusammenhang mit dem Datenschutz, die personenbezogenen Daten des Verantwortlichen betreffen, zu informieren, nachdem er den betreffenden Vorfall festgestellt hat bzw. Kenntnis davon erlangt hat.

(vi) Der Auftragsbearbeiter ist verpflichtet, alle daraus resultierenden angemessenen Empfehlungen innerhalb der vereinbarten Frist umzusetzen. Für den Fall, dass es nach den angemessenen Empfehlungen des Verantwortlichen notwendig sein sollte, dass Personal des Verantwortlichen in den Einrichtungen des Auftragsbearbeiters zugegen ist, verpflichtet sich der Auftragsbearbeiter, die Anwesenheit vom Personal des Verantwortlichen auf Kosten des Verantwortlichen zu ermöglichen.

14. Definitionen

In diesem Auftragsbearbeitungsvertrag gilt Folgendes:

"***Zugang bzw. Fernzugang***" bedeutet die Tätigkeit oder Fähigkeit des Erstellens, Abrufens, Änderns, Weitergebens, Speicherns oder *Bearbeitens* von Personenbezogenen Daten, Assets, Medien und Datenträgern des VERANTWORTLICHEN oder des AUTRAGSBEARBEITERS.

"**Vertrag**" bedeutet der im einleitenden Teil genannte *Vertrag* zwischen den *Parteien*.

"**Angemessene Sicherheitsvorkehrungen**" umfasst alle Massnahmen zum Kompensieren eines fehlenden Schutzes in einem konkreten Drittland, in das *Personenbezogene Daten* exportiert werden, in dem kein angemessenes Schutzniveau besteht, bzw. jegliche Massnahmen zum Kompensieren eines fehlenden Schutzes in Bezug auf jede Art von *Bearbeitung Personenbezogener Daten*. Die zuständigen Aufsichtsbehörden betroffener Jurisdiktionen bestimmen die Angemessenheit einiger Drittländer.

"**Vertrauliche Informationen**" bedeutet alle Informationen nicht-öffentlicher Art in Bezug auf eine Partei oder eines ihrer *Konzernmitglieder*, die durch eine Partei oder eines ihrer *Konzernmitglieder* (hierin "**Offenlegende Partei**" genannt) gegenüber der anderen Partei oder einem ihrer *Konzernmitglieder* (hierin "Erhaltende Partei" genannt) in mündlicher, schriftlicher, elektronischer oder beliebiger sonstiger Form offengelegt werden oder der Erhaltenden Partei während der Erbringung von *Dienstleistungen* gemäss *Vertrag* anderweitig zur Kenntnis gelangen. *Vertrauliche Informationen* umfassen unter anderem technologische oder organisatorische Prozesse, Kunden, Personal, geschäftliche Aktivitäten, Datenbanken, geistiges Eigentum, die Bestimmungen und Konditionen beliebiger Verträge und andere damit zusammenhängende Informationen sowie alle sonstigen Informationen, bei denen angemessenerweise oder üblicherweise von einem vertraulichen oder anderweitig sensiblen Charakter auszugehen ist, unabhängig davon, ob sie konkret als vertraulich gekennzeichnet sind oder nicht wie z.B. *Fertigungs- und Geschäftsgeheimnisse*. *Vertrauliche Informationen* beinhalten keine Informationen, die (i) der Erhaltenden Partei bereits vor der Offenlegung auf rechtmässige Weise ohne Vertraulichkeitsverpflichtung vorgelegen haben und durch die Erhaltende Partei weder direkt noch indirekt von der Offenlegenden Partei erlangt wurden, oder (ii) aufgrund einer durch den Eigentümer der betreffenden Informationen genehmigten Offenlegung allgemein verfügbar sind oder werden, oder (iii) der Erhaltenden Partei auf rechtmässige Weise durch eine Drittpartei zur Verfügung gestellt wurden, die zur Weitergabe oder Offenlegung derselben auf nicht-vertraulicher Grundlage befugt ist, oder (iv) durch die Erhaltende Partei auf eigenständige Weise und ohne Bezugnahme auf *Vertrauliche Informationen* der Offenlegenden Partei nachweislich selbst entwickelt werden.

"**VERANTWORTLICHER**" bedeutet die natürliche oder juristische Person, Behörde, Agentur oder eine beliebige sonstige Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der *Bearbeitung* von *Personenbezogenen Daten* entscheidet.

"**Gesetze und Vorschriften zum Datenschutz**" bedeutet Gesetze und Vorschriften zum Datenschutz und/oder zur *Bearbeitung Personenbezogener Daten* in Bezug auf den VERANTWORTLICHEN und den AUTRAGSBEARBEITER wie insbesondere aber nicht abschliessend die der Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der *Bearbeitung Personenbezogener Daten* und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG (Allgemeine Datenschutzverordnung) und des Schweizerischen Bundesgesetzes über den Datenschutz vom 25. September 2020 einschliesslich der für jeden VERANTWORTLICHEN und/oder jedes *Konzernmitglied* des VERANTWORTLICHEN geltenden nationalen Gesetze und Vorschriften zum Datenschutz.

"**Betroffene Person(en)**" bedeutet eine identifizierte oder identifizierbare natürliche Person, die auf direkte oder indirekte Weise identifiziert werden kann, insbesondere unter Bezugnahme auf einen Identifikator, wie beispielsweise einen Namen, eine Identifikationsnummer, eine IP-Adresse, Ortsdaten, einen Online-Identifikator oder einen oder mehrere Faktoren, die sich konkret auf die physische,

physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität der betreffenden natürlichen Person beziehen, vorbehaltlich dessen, dass *Betroffene Personen* (i) auch andere Personen als lebende Einzelpersonen sowie (ii) juristische Personen, soweit die *Bearbeitung Personenbezogener Daten* einer juristischen Person durch die Gesetze oder Vorschriften zum Datenschutz reguliert wird, einschliesst.

"**EU-Standardvertragsklauseln**" Die Standardvertragsklauseln gemäss dem Beschluss der Europäischen Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsbearbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU) wurde durch die Europäische Kommission mit Wirkung auf 27. September 2021 mit dem Durchführungsbeschluss (EU) 2021/914 vom 4. Juni 2021 aufgehoben und durch die Standardvertragsklauseln ersetzt, die im Anhang desselben Durchführungsbeschlusses 2021/914/EU zu finden sind.

"**Personenbezogene Daten des VERANTWORTLICHEN**" schliesst unter anderem Personenbezogene Daten der *Vertreter*, Kunden und/oder *AUFTRAGSDATEERARBEITER*, des VERANTWORTLICHEN ein.

"**Konzernmitglied**" bedeutet des VERANTWORTLICHEN oder des AUTRAGSBEARBEITERS Tochtergesellschaft und Konzerngesellschaften.

"**Fertigungs- und Geschäftsgeheimnis**" bedeutet die gesetzliche und vertragliche Verpflichtung, keine Informationen offenzulegen, die sich auf irgendeinen durch den VERANTWORTLICHEN geheimgehaltenen Geschäftsbereich beziehen.

"**Partei(en)"** bedeutet die im Vertrag definierte(n) Partei(en), einschliesslich der genehmigten Abtretungsempfänger und Nachfolger der betreffenden Partei(en).

"**Personenbezogene Daten**" bedeutet jegliche Informationen über eine betroffene Person, einschliesslich gesundheitsbezogener Daten und genetische Daten gemäss diesem Vertrag und Gesetze und Vorschriften zum Datenschutz.

"**Bearbeitung / Bearbeiten**" bedeutet jegliche Aktivitäten oder Gruppen von Aktivitäten, die in Bezug auf *Personenbezogene Daten* oder Sätze *Personenbezogener Daten* ausgeführt werden, unabhängig davon, ob unter Verwendung automatisierter Mittel oder nicht, wie beispielsweise die Erfassung, Aufzeichnung, Organisation, Gliederung, Speicherung, Anpassung oder anderweitige Veränderung, Abfrage, Einsichtnahme, Nutzung, Offenlegung durch Weitergabe, Verbreitung oder anderweitige Bereitstellung, Abgleichung oder Kombination, Beschränkung, Löschung oder Vernichtung von Daten oder der *Zugang* zu ihnen.

"**AUFTRAGSBEARBEITER**" bedeutet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die *Personenbezogene Daten* im Auftrag des VERANTWORTLICHEN *Bearbeitet*.

"**Pseudonymisierung**" bedeutet die *Bearbeitung Personenbezogener Daten* in der Weise, dass *Personenbezogenen Daten* nicht länger einer *Betroffenen Personen* ohne Nutzung zusätzlicher Informationen zugeordnet werden können, unter der Bedingungen, dass die betreffenden zusätzlichen Informationen gesondert verwahrt werden und Gegenstand technischer und organisatorischer Massnahmen sind, durch die sichergestellt wird, dass keine Re-Identifikation erfolgen kann.

"**Vertreter**" umfasst die Belegschaft, Direktoren, Führungskräfte, Mitarbeiter, Erfüllungsgehilfen, Berater, Auftragnehmer, *Subunternehmer* sowie jegliche sonstigen Arten von ermächtigten Vertretern und Beratern einer Partei, sofern zutreffend, bzw., je nach Fall, Personal.

"**Relevante Weitergabe**" bedeutet eine Weitergabe *Personenbezogener Daten* an eine Drittpartei, die sich in einem Land befindet, das (für die Zwecke dieses Anhangs) keine *Angemessenen Sicherheitsvorkehrungen* bietet.

“**Dienstleistungen**” umfasst (1) die im *Vertrag* beschriebenen *Dienstleistungen*, Aufgaben und Zuständigkeiten, darin eingeschlossen die Bereitstellung von Liefergegenständen, sofern zutreffend, gegebenenfalls einschliesslich jeglicher Gewährleistungsbehelfe, die dem VERANTWORTLICHEN und/oder ihre *Tochtergesellschaft* durch den AUTRAGSBEARBEITER oder die Gesellschaft des AUTRAGSBEARBEITERS unentgeltlich eingeräumt werden; (2) *Dienstleistungen*, Aufgaben und Zuständigkeiten, die einen angemessenen Bezug zum *Vertrag* aufweisen und in den Monaten vor Beginn der Erbringung der jeweiligen *Dienstleistungen* durch oder für den LIEFERNANTEN, seine *Tochtergesellschaft* oder Dritt-AUFTRAGSBEARBEITER ausgeführt werden, deren *Dienstleistungen*, Aufgaben oder Zuständigkeiten im Ergebnis durch den *Vertrag* entfallen, was selbst für den Fall gilt, dass dies in keiner im *Vertrag* ausdrücklich festgehalten ist; und (3) jegliche *Dienstleistungen*, Aufgaben und Zuständigkeiten, die zwar nicht ausdrücklich in irgendeiner der *Vertragen* festgehalten sind, die jedoch im Hinblick auf die ordnungsgemässe Ausführung und Erbringung der unter (1) und (2) beschriebenen *Dienstleistungen* erforderlich sind.

“**Subunternehmer**” bedeutet jegliche durch den AUTRAGSBEARBEITER beauftragten Erfüllungsgehilfen, Auftragnehmer oder sonstigen Drittparteien.

“**Tochtergesellschaft(en)**” bedeutet eine teilweise (mehr als 51% der Stimmrechte) oder vollständig kontrollierte *Tochtergesellschaft*, Zweigniederlassung, Beteiligungsgesellschaft oder Vertretung.

Anlage 3: Template zur Meldung von Datenschutzverletzungen

Auftragsbearbeitungsvertrag zum Hauptvertrag zwischen smino AG, Werkstrasse 20, 8645 Rapperswil-Jona [«AUFTRAGSBEARBEITER»] und dem VERANTWORTLICHEN.

Anweisungsrichtlinien

☐ [Gesellschaft] ist **Verantwortlicher** der Daten

Verletzung des Datenschutzes bei:

☐ [Gesellschaft]	→ Meldung [Gesellschaft] an die zuständige Aufsichtsbehörde + betroffene Person
☐ AUFTRAGSBEARBEITER der [Gesellschaft]	→ Meldung des AUFTRAGSBEARBEITERs an [Gesellschaft] → Meldung [Gesellschaft] an die zuständige Aufsichtsbehörde + betroffene Person

☐ [Gesellschaft] ist AUFTRAGSBEARBEITER der Daten

Verletzung des Datenschutzes bei:

☐ [Gesellschaft]	→ Meldung [Gesellschaft] an den Verantwortlichen
☐ Sub-AUFTRAGSBEARBEITER von [Gesellschaft]	→ Meldung des Sub-AUFTRAGSBEARBEITERs an [Gesellschaft] → Meldung [Gesellschaft] an den Verantwortlichen

Angaben über die meldende Organisation oder den meldenden Verantwortlichen

Organisation/Abteilung, in welcher die Datenschutzverletzung geschehen ist:

Funktion: ☐ Verantwortlicher ☐ AUFTRAGSBEARBEITER ☐ .....

Name der Organisation: .....

Adresse der Organisation: .....

Betroffene Abteilung: .....

Betroffene Systeme: .....

Website (falls betroffen): .....

Name des DSB: .....

Kontaktinfo des DSB: .....

Meldende Person

Vollständiger Name: .....

Funktion: .....

Kontaktinfo: .....

Verantwortlicher der betroffenen Daten [*falls, Datenschutzverletzung nicht beim Verantwortlichen*]

Name der Organisation: .....

Adresse der Organisation: .....

Name des DSB: .....

Kontaktinfo des DSB: .....

Information über die Datenschutzverletzung

Type

☐ Datendiebstahl ☐ Datenverlust ☐ Datenmanipulation
☐ Cyberattacke ☐ Ransomware ☐ Malware
☐ Phishing ☐ Falschversand von Daten ☐ Fehlerhafte Datenlöschung

☐ .....

Zeitliche Angaben der Datenschutzverletzung

Datum, Zeit: .....

Zeitspanne: .....

Zeitpunkt der Entdeckung: .....

Beschrieb

[*Situation? / Ort? / Wie wurde die Datenschutzverletzung entdeckt? / Wer wurde bereits informiert?*]

.....

.....

.....

Betroffene Personen und betroffene Personendaten

Kategorie der betroffenen Person

☐ Arbeitnehmer ☐ Klient / Kunde ☐ Lieferant

☐ Benutzer (Dienstleistungen) ☐ Benutzer (Website) ☐ Minderjährige

☐ .....

Kategorie der betroffenen Personendaten

☐ Name	☐ Postadresse	☐ Geburtsdatum
☐ ID/Passnummer	☐ Steueridentifikationsnummer	☐ Sozialversicherungsnummer
☐ E-Mail Adresse	☐ Benutzername	☐ Passwort
☐ Aufenthaltsort/GPS-Daten	☐ Fotos/Videos	☐ Biometrische Daten
☐ Bankdaten	☐ Kreditkarteninformation	☐ Finanzielle Informationen
☐ Gesundheitsdaten	☐ Berufsgeheimnis	☐ Wirtschaftliche Geheimnisse
☐ Strafrechtliche Daten	☐ Sexualität	☐ Politische Meinung
☐ Ethnie	☐ Religion	

☐ .....

Ausmasse der Datenschutzverletzung

Anzahl der betroffenen…

Personen: ..... Datensätze: .....

Konsequenzen der Datenschutzverletzung

Allgemeine Konsequenzen

eingetreten (e) / möglich (m)

e	*m*		*e*	*m*		*e*	*m*	
☐	☐	Datenverlust	☐	☐	Vertraulichkeitsverletzung	☐	☐	Zugangsbeschränkungen
☐	☐	Datenveröffentlichung						

☐ ☐ .....

Konsequenzen für die betroffenen Personen

eingetreten (e) / möglich (m)

e	*m*		*e*	*m*		*e*	*m*	
☐	☐	Finanzieller Schaden	☐	☐	Rufschädigung	☐	☐	Identitätsdiebstahl/Betrug
☐	☐	Geheimnisverletzung	☐	☐	Soziale Konsequenzen	☐	☐	Wirtschaftliche Folgen

☐ ☐ .....

Prävention

Massnahmen

ergriffen (e) / vorgeschlagen (v)

e	*v*		*e*	*v*		*e*	*v*	
☐	☐	System heruntergefahren	☐	☐	System getrennt	☐	☐	Beweissicherung
☐	☐	Meldung an Verantwortlichen	☐	☐	Meldung an betroffene Person	☐	☐	Meldung an Polizei / Aufsichtsbehörde

☐ ☐ .....

Sollte zum Zeitpunkt der Mitteilung die eine oder andere Tatsache noch nicht ermittelbar sein, so kann die meldende Organisation eine weitere Meldung zu einem späteren Zeitpunkt erstatten.

Rechtsverbindliche Bestätigung der Richtigkeit und Vollständigkeit der Angaben:

Ort, Datum: …….....

……... ……...

Geschäftsleitung der meldenden Organisation DSB der meldenden Organisation