Auftragsverarbeitungsvertrag

zwischen

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

plazz AG
Bahnhofstraße 5a
D-99084 Erfurt

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

Präambel

Diese Vereinbarung stellt sicher, dass die plazz AG als Dienstleister für Event- und Community-Plattformen personenbezogene Daten im Rahmen der Zusammenarbeit mit dem Auftraggeber sicher, transparent und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) verarbeitet. Sie dient dem Schutz der betroffenen Daten sowie einer klaren und vertrauensvollen Aufgabenteilung zwischen beiden Parteien.

§ 1 Begriffsbestimmungen

Für in dieser Vereinbarung benutzte Begriffe, für die Art. 4 DS-GVO eine Begriffsbestimmung vorsieht, gilt diese gesetzliche Definition in der im Zeitpunkt des Vertragsschlusses geltenden Fassung auch für diesen Vertrag.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Datenschutz-Aufsichtsbehörde für den Auftragnehmer ist:

Thüninger Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Häßlerstrasse 8
D - 99096 Erfurt

(2) Der Auftraggeber benennt dem Auftragnehmer auf Anfrage seine zuständige Datenschutz-Aufsichtsbehörde.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Datenschutz-Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich von Event & Community Plattformen auf Grundlage des Vertrags zu DEAL/Angebots-Nummer _2025/_____ ggf. beauftragt am _____ („Hauptvertrag“). Dabei erhalten der Auftragnehmer und seine Beschäftigten oder durch den

Auftragnehmer Beauftragte Zugriff auf personenbezogene Daten und verarbeiten diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und, sofern vorhanden, aus der dazugehörigen Leistungsbeschreibung) sowie aus der ***Anlage 1*** zu diesem Vertrag. Der Auftraggeber stellt sicher, dass die Verarbeitung der personenbezogenen Daten im Einklang mit den geltenden Datenschutzbestimmungen erfolgt.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht über die Laufzeit des Hauptvertrages hinausgehende Verpflichtungen ergeben. Sich aus diesem Vertrag ergebende Kündigungsrechte bleiben von der vorstehenden Regelung unberührt.

(4) Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat. Dies gilt auch für nachfolgende Verträge zwischen den Parteien, unabhängig von einer abweichenden DEAL-Nummer, sofern diese Verträge den gleichen Leistungsgegenstand betreffen und nichts Abweichendes geregelt ist.

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

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers verarbeiten. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern ihm dies rechtlich gestattet ist.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung und Löschung von Daten sowie auf die Einschränkung der Verarbeitung. Die weisungsberechtigten Personen oder Abteilungen ergeben sich aus ***Anlage 4***. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Sofern ein Vertragspartner keine weisungsberechtigten Personen oder Abteilungen benennt, gelten sämtliche dokumentierten Weisungen, die in seinem Verantwortungsbereich erteilt wurden, als von ihm akzeptiert und verbindlich.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer, je nach Auftragsumfang, Zugriff auf die in ***Anlage 1*** näher spezifizierten personenbezogenen Daten der ebenfalls in ***Anlage 1*** näher spezifizierten betroffenen Personen. Diese Daten umfassen die in ***Anlage 1*** aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht ohne entsprechende Weisung an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen in Papierform und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in ***Anlage 2*** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Abs. 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen, welche in ***Anlage 2*** genauer spezifiziert sind. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung welche Maßnahmen getroffen werden und die Umsetzung der Maßnahmen offen.

Eine Verbesserung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten und der Auftraggeber über wesentliche Veränderungen unverzüglich informiert wird.

(3) Datenschutzbeauftragter beim Auftragnehmer ist: ***PRILUTIONS Rechtsanwaltsgesellschaft mbH mit Sitz in 99090 Erfurt***. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Datenschutz-Aufsichtsbehörde mit. Ein Wechsel in der Person des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b DS-GVO), über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren und mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen der Mitarbeiter auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen bei den Verarbeitungstätigkeiten, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers oder Verdacht auf sonstige sicherheitsrelevante Vorfälle beim Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, die für den Auftraggeber relevante Verarbeitungen oder Sachverhalte betreffen. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält, soweit möglich, folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher nachteiliger Folgen für die betroffene(n) Person(en), informiert hierüber den Auftraggeber, ersucht ihn um weitere Weisungen und erteilt dem Auftraggeber jederzeit weitere Auskünfte, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

(3) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber liegt.

(4) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(5) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(6) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO und ggf. bei der vorherigen Konsultation der Datenschutz-Aufsichtsbehörden gem. Art. 36 DS-GVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers, sofern möglich, nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß ***Anlage 2*** erforderlich sind.

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

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Um unseren Kunden stets die bestmöglichen Dienstleistungen zu bieten, arbeitet die plazz AG mit sorgfältig ausgewählten Subunternehmern zusammen. Diese werden nach strengen Datenschutzvorgaben ausgewählt, um ein hohes Maß an Sicherheit und Verlässlichkeit zu gewährleisten. Im Rahmen dieser Zusammenarbeit werden die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen unter Einschaltung der in ***Anlage 3*** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Diese werden durch einen Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats zur Einhaltung derselben Datenschutzpflichten verpflichtet, wie sie im Auftragsverarbeitungsvertrag zwischen dem Auftraggeber und dem Auftragnehmer gemäß Art. 28 Abs. 3 DSGVO festgelegt sind. Insbesondere sind dabei hinreichende Garantien dafür sicherzustellen, dass geeignete technische und organisatorische Maßnahmen getroffen werden, die gewährleisten, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Subunternehmers. Der Auftragnehmer stellt sicher, dass bei Datenübermittlungen in Drittländer die Voraussetzungen des Kapitel 5 der DSGVO eingehalten werden, insbesondere Angemessenheitsbeschlüsse oder Standardvertragsklauseln (SCC) samt Transfer Impact Assessment vorliegen und weist dies auf Nachfrage dem Auftraggeber nach.

Vor der Begründung von weiteren Unterauftragsverhältnissen informiert der Auftragnehmer den Auftraggeber in Textform mit einer Frist von vier Wochen. Der Auftraggeber kann gegen die Änderung nur aus wichtigem Grund Einspruch erheben. Der Einspruch hat binnen 14 Kalendertagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Ein wichtiger Grund auf Seiten des Auftragnehmers liegt insbesondere vor, wenn der Subunternehmer seinen Sitz nicht in einem Land hat, das Mitglied der EU/des EWR ist oder zu dem die Kommission einen Angemessenheitsbeschluss nach Art. 45 DS-GVO erlassen hat.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Subunternehmerverhältnisse i.S.v. Abs. 1 dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers nach Art. 12–22 sowie 32 und 36 DS-GVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Der Auftragnehmer stellt den Auftraggeber von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DS-GVO auferlegten Pflicht oder wegen der Nichtbeachtung oder Verletzung einer in dieser Vereinbarung festgelegten Pflicht oder einer vom Auftraggeber gesondert erteilten Weisung geltend machen.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn/soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Abs. 5 DS-GVO.

(4) Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 12 Kosten

(1) Soweit der Auftragnehmer den Auftraggeber nach Maßgabe dieses Vertrags bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen unterstützt, erfolgt diese Unterstützung grundsätzlich ohne gesonderte Vergütung.

(2) In folgenden Fällen kann der Auftragnehmer jedoch eine angemessene Vergütung seines Aufwands verlangen:

a) Unterstützung bei der Erstellung und Pflege des Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und einer vorherigen Konsultation der Datenschutz-Aufsichtsbehörde gemäß Art. 36 DS-GVO (§ 7).

b) Durchführung oder Unterstützung von Kontrollen durch den Auftraggeber gemäß § 8.

c) Unterstützung bei der Bearbeitung von Anfragen betroffener Personen gemäß § 10.

(3) Eine Vergütung kann nur verlangt werden, soweit der entstandene Aufwand über das übliche Maß hinausgeht und nicht durch allgemeine vertragliche Pflichten des Auftragnehmers abgedeckt ist. Die Höhe der Vergütung richtet sich nach den marktüblichen Stundensätzen des Auftragnehmers, sofern keine anderweitige Vereinbarung zwischen den Parteien getroffen wurde.

(4) Der Auftragnehmer wird den Auftraggeber vor der Erbringung kostenpflichtiger Unterstützungsleistungen auf die entstehenden Kosten hinweisen und eine schriftliche oder textliche Zustimmung einholen.

§ 13 Außerordentliches Kündigungsrecht

Bei einfachen Verstößen, die weder vorsätzlich noch grob fahrlässig erfolgen, erhält der Auftragnehmer zunächst die Möglichkeit, den Mangel innerhalb einer angemessenen Frist zu beheben. Sollte der Verstoß innerhalb dieser Frist nicht behoben werden, kann der Auftraggeber weitere Maßnahmen ergreifen, einschließlich einer außerordentlichen Kündigung.

Unabhängig davon hat der Auftraggeber das Recht, den Hauptvertrag fristlos ganz oder teilweise zu kündigen, wenn der Auftragnehmer seinen vertraglichen Pflichten nicht nachkommt, gegen die Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verstößt oder eine Weisung des Auftraggebers nicht ausführen kann oder will.

§ 14 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen in Papierform, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Die Herausgabe- bzw. Vernichtungsverpflichtung betrifft auch etwaige Datensicherungen beim

Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

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

§ 15 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass dem Auftragnehmer kein Zurückbehaltungsrecht hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger zusteht.

(2) Änderungen und Ergänzungen dieses Vertrags, die Erklärung einer Kündigung sowie die Abänderung dieser Klausel bedürfen zu ihrer Wirksamkeit der Schriftform (§ 126 Abs. 1, 2 BGB). Die Ersetzung der Schriftform durch die elektronische Form (§§ 126 Abs. 3, 126 a BGB) oder die Textform (§ 126 b BGB) ist ausgeschlossen. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Erfurt.

Anlagen

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Anlage 4 – Weisungsberechtigte Personen

Unterschriften

	Erfurt,
_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber, vertreten durch	Auftragnehmer, vertreten durch Jürgen Mayer - CEO plazz AG

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Betroffene Personen:

- Projektbeteiligte (Organisatoren, Sprecher, Sponsoren, Aussteller)
- Besucher/Teilnehmer
- Beschäftigte und freie Mitarbeiter, Alumni
- (Vereins/Gremien)-Mitglieder
- Kunden
- Lieferanten/ Dienstleister
- Geschäftspartner

Personenbezogene Daten/Datenkategorien:

Die folgenden personenbezogenen Daten werden dann verarbeitet, wenn sie durch den Auftraggeber erfasst werden (***freiwillige*** Angaben des Auftraggebers):

- Stammdaten (ID, Vorname, Nachname, Geburtsdatum)
- Kontaktdaten (Adresse, E-Mail-Adresse, Telefonnummer)
- Zugangsdaten (Nutzerkennung, Passwort)
- Daten aus dem Beschäftigungsverhältnis (Firma, Position, Stadt, Gruppenzugehörigkeit, Personalnummer)
- Reisedaten (Reisedatum, Personalausweisnummer für Flugbuchungen, Reisezeit)
- Trackingdaten (z.B. App-Abstürze, Opt-Out verfügbar, (indiv.) App-Nutzung - insofern vom Auftraggeber gewünscht)
- Bild- und Videodaten (Profilbild, Fotos und Videos)
- Eigener User Generated Content (z.B. Notizen)
- Geteilter User Generated Content (Kommunikationsdaten wie z.B. abgegebene Bewertungen, Chatnachrichten, in der App hinterlegte Termine, Posts und Likes)
- Sonstige Daten (Beschreibungstexte, Kleidergröße, _____)

Besondere personenbezogene Daten/Datenkategorien:

Die folgenden besondere personenbezogenen Daten werden dann verarbeitet, wenn sie durch den Auftraggeber erfasst werden (***freiwillige*** Angaben des Auftraggebers):

- Religion, Einschränkungen, Allergien/Unverträglichkeiten
- _____

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Im folgenden Dokument wird ein detailliertes Verzeichnis der technischen und organisatorischen Maßnahmen (TOM) dargestellt, welche der Auftragsverarbeiter zum Schutz der vertragsgegenständlichen personenbezogenen Daten umsetzt. Die Maßnahmen dienen gemeinsam und funktionsübergreifend den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, weshalb auf die wiederholte Aufzählung von schutzzielübergreifenden Maßnahmen verzichtet wurde.

1. Zutrittskontrolle

Unter dem Begriff Zutrittskontrolle versteht man jene Maßnahmen, die gewährleisten, dass ausschließlich autorisierte Personen Zutritt zu Räumlichkeiten oder Anlagen haben, in denen personenbezogene Daten verarbeitet werden, um Risiken durch physischen Zugriff Dritter zu vermeiden. Im nachfolgenden Abschnitt werden die spezifischen Maßnahmen und Strategien erläutert, die der Auftragnehmer implementiert hat, um eine effektive Zutrittskontrolle zu gewährleisten:

- Protokollierung und Begleitung aller Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Dokumentation von Zutrittsrechten
- dokumentiertes Verfahren für die Vergabe/ den Entzug von Zutrittsrechten
- Zutrittsrechte „Serverraum“ auf IT Ops begrenzt
- Alarmanlage
- Klingelanlage mit Kamera
- Videoüberwachung der Zugänge (Türen und Fenster)
- Absicherung der Gebäudeschächte
- Türen mit Außenknauf
- Transpondersystem für Eingangs- und Nebentüren
- Festlegung von Sicherheitszonen/Sperrbereichen
- Closed-Shop-Betrieb für Datenverarbeitungs-, Telekomunikations-Systeme
- Automatische Zugangskontrolle
- Schlüsselregelung
- Empfang/Rezeption

2. Zugangskontrolle

Die Zugangskontrolle befasst sich mit der Sicherung digitaler Ressourcen und gewährleistet, dass nur berechtigte Personen Zugriff auf bestimmte Daten, Systeme oder Anwendungen haben. So wird der unberechtigte Zugriff auf personenbezogene Daten verhindert und sichergestellt, dass diese nicht gelesen, kopiert, verändert oder gelöscht werden können. Im folgenden Abschnitt werden die spezifischen

Maßnahmen und Strategien erläutert, die der Auftragnehmer implementiert hat, um eine zuverlässige Zugangskontrolle zu gewährleisten:

- Zuordnung von Benutzerrechten
- Dokumentation von Zugangsberechtigungen
- Passworthistorie zur Vermeidung von Weiterverwendung alter Passwörter
- Passwort-Richtlinie (regelmäßige Änderung, Mindestlänge, Komplexität)
- Login mit biometrischen Daten
- Individuelle Vergabe von Passwörtern / Zentrale Passwortvergabe (für die Erstanmeldung)
- Beschränkte Anzahl
- Verschlüsselte Aufbewahrung und Übertragung von Passwörtern
- Sichere Aufbewahrung von Administrationspasswörtern
- Sichere Aufbewahrung von Schlüsseln für Kryptographie-Verfahren
- Authentifikation mit Benutzername / Passwort
- 2-Faktor-Authentifizierung / Teilnehmerkennung
- Protokollierung der Systemnutzung und Protokollauswertung
- Automatische Sperrung von Bildschirmen bei Arbeitsunterbrechungen (passwortgeschützt)
- Einsatz von VPN-Technologie
- Automatische Protokollierung von allen Aktivitäten auf Datenverarbeitungsanlagen
- Zugangskontrollsysteme an Räumen mit IT-Systemen
- Sicherheitsschlösser
- Einsatz von Anti-Viren-Software (Server / mobile Geräte / Clients)
- Verschlüsselung von Datenträgern in Laptops/Notebooks/Tablets und Smartphones
- Laptops außerhalb der Geschäftszeiten unter Verschluss
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- BIOS-Schutz (separates Passwort)

3. Zugriffskontrolle

Das Hauptziel der Zugriffskontrolle ist es, sicherzustellen, dass Daten nicht nur vor unberechtigten Zugriffen geschützt sind, sondern auch, dass berechtigte Nutzer genau den Zugriff erhalten, den sie benötigen – nicht mehr und nicht weniger. In diesem Abschnitt werden die Verfahren und Technologien vorgestellt, die der Auftragnehmer verwendet, um diese granulare Steuerung und Überwachung des Datenzugriffs zu gewährleisten:

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte)
- Dokumentation von Zugriffsberechtigungen
- Jährliche Überprüfung der Zugriffsrechte durch internes Systemaudit
- Verwaltung der Rechte durch IT Ops

- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Passwort-Richtlinie (regelmäßige Änderung, Mindestlänge, Komplexität)
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Physische Löschung von Datenträgern vor Wiederverwendung
- Datenschutzkonforme Vernichtung von Datenträgern
- Verschlüsselung von Datenträgern
- Verbot von mobilen externen Datenträgern
- Sichere Aufbewahrung der Datenträger außerhalb der Geschäftszeiten (unter Verschluss)
- Differenzierung der Zugriffsberechtigung in Dateien, Anwendungsprogramme und Server/IT
- Differenzierung der Verarbeitungsmöglichkeiten in Lesen, Ändern, Löschen
- Test und Freigabe von Anwendungssoftware vor der Nutzung
- Akten-Schredder
- Datenschutztresor

4. Weitergabekontrolle/Übermittlungskontrolle

Die Weitergabekontrolle oder Übermittlungskontrolle stellt sicher, dass personenbezogene Daten beim Transfer zwischen unterschiedlichen Stellen oder bei der Offenlegung gegenüber Dritten stets geschützt und nur gemäß den geltenden Datenschutzbestimmungen übermittelt werden. Dies verhindert nicht nur unbeabsichtigte Datenlecks, sondern gewährleistet auch, dass Daten nur an diejenigen weitergegeben werden, die dazu berechtigt sind. Im folgenden Abschnitt werden die Mechanismen, Richtlinien und Technologien erörtert, die beim Auftragnehmer implementiert sind, um eine sichere und regelkonforme Datenübermittlung zu gewährleisten:

- Berechtigungskonzept für Netzwerkfreigaben und Zugriffsberechtigungen auf Ordner und Dateien für einzelne Benutzergruppen (jährliche Prüfung)
- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Einsatz von Sicherungsmechanismen bei der Übermittlung von Daten (alle Protokolle via VPN/IPsec gesichert, E-Mail mit S/MIME oder PGP, SFTP)
- Datenschutzkonforme Vernichtung von Datenträgern
- Schriftliche Verpflichtungen zum Datenschutz von externen Dienstleistern
- Beaufsichtigung externer Dienstleister während ihrer Tätigkeit
- Einsatz von Firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Virtual Private Network (VPN), Content Filter
- IT-Systeme befinden sich in verschlossenen Räumen / Sperrung der Serverkonsolen
- Passwortwechsel nach Bekanntgabe an einen externen
- Ausschließlich fallbezogene und genehmigte Freigaben von Fernwartungen

- Vertraglich geregelte Maßnahmen zum Schutz von Daten/Informationen bei Fernwartungen
- Entzug von Zugangsberechtigungen bei Ausscheiden eines Mitarbeiters
- Nutzung von Signaturverfahren
- Sorgfalt bei Auswahl von Transport- Personal und Fahrzeuge
- Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
- Persönliche Übergabe mit Protokoll
- Sicherer Transportbehälter

5. Eingabekontrolle

Die Eingabekontrolle dient dazu, sicherzustellen, dass bei der Erfassung, Änderung oder Löschung von Daten stets nachvollziehbar bleibt, wer welche Daten zu welchem Zeitpunkt eingegeben oder modifiziert hat. In diesem Abschnitt beleuchten wir die Prozesse und Technologien, die beim Auftragnehmer eingesetzt werden, um die Eingabe und Überprüfung von Daten zu steuern und deren Qualität und Integrität zu gewährleisten:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Logdaten, Tickets und Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Einsatz eines Schadsoftwareschutzes mit automatischen Updates
- Regelmäßige und zeitnahe Updates für Betriebssysteme und Anwendungssysteme
- getrennte Speicherung von Daten und Programmen (Verzeichnisse)
- Überprüfung der Integrität und Installation von erhaltenen Programmen
- Vollständige Netzwerkdokumentation
- Dokumentation von Wartungs-, Fernwartungs- und Reparaturarbeiten
- Dauerhafte Überprüfung von Fernwartungsarbeiten durch dauerhaften Mitschnitt der Remotesession
- Datenschutzkonforme Löschung von beschriebenen Datenträgern vor erneuter Nutzung
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

6. Auftragskontrolle/Vertragskonformitätskontrolle

Die Auftragskontrolle, auch als Vertragskonformitätskontrolle bezeichnet, sorgt dafür, dass die Verarbeitung personenbezogener Daten durch Dritte im Einklang mit den geltenden Datenschutzbestimmungen und den vereinbarten vertraglichen Verpflichtungen steht.

Sie gewährleistet, dass externe Partner Daten nicht eigenmächtig nutzen oder verändern und dass die Datenschutzstandards durchgehend eingehalten werden. Im folgenden Abschnitt erläutern wir die Maßnahmen und Strategien, die beim Auftragnehmer Unternehmen werden, um eine konforme und sichere Datenverarbeitung im Auftragsverhältnis zu sicherzustellen:

- Formalisierte Auftragserteilung
- Strenge Auswahl des Dienstleisters
- Vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Changemanagement Prozess bei Änderungen im Verfahrensablauf/Programmänderungen durch den Auftragnehmer
- Fernwartung/Fernadministration nur nach Ereignisauslöser vom Auftraggeber (Protokollierung)
- Schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- Regelung zum Einsatz weiterer Subunternehmer

7. Verfügbarkeitskontrolle/Wiederherstellbarkeit

Die Verfügbarkeitskontrolle konzentriert sich darauf, sicherzustellen, dass Daten und Systeme zu jeder Zeit zugänglich sind, insbesondere wenn sie benötigt werden, und gleichzeitig vor unbeabsichtigten oder böswilligen Beeinträchtigungen geschützt sind, sei es durch technische Störungen, Naturkatastrophen oder gezielte Angriffe. Es geht hierbei nicht nur um den Schutz vor Datenverlust, sondern auch um die schnelle Wiederherstellung von Daten und Systemen im Falle eines Ausfalls.
In diesem Abschnitt werden die Maßnahmen und Techniken vorgestellt, die beim Auftragnehmer implementiert sind, um die durchgängige Verfügbarkeit von Daten sicherzustellen und Risiken zu minimieren:

- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsfilter
- Back-up-Rechenzentrum
- Notfall- und Krisenmanagement (BCM)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Meldesystem bei Alarm innerhalb der Serverräume

- Rufbereitschaft im Katastrophenfall
- Archivordnung mir beschränktem Zugang zum Archivbereich
- Erstellen eines Backup- & Recoverykonzepts
- Tägliche und wöchentliche Datensicherung
- Erstellung und Prüfung von Backup-Verfahren
- Dokumentation des Backup-Verfahrens
- Spiegelung von Festplatten mittels Raid-Verfahren
- Videoüberwachung im Serverraum
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- Beachtung gesetzlicher Aufbewahrungsfristen
- Testen der Wiederherstellung

8. Datentrennungskontrolle/Mandantentrennungskontrolle

Die Datentrennungskontrolle stellt sicher, dass Datenbestände gemäß ihres spezifischen Verarbeitungszwecks voneinander isoliert werden. Dies gewährleistet nicht nur die Wahrung der Vertraulichkeit und Integrität der Daten, sondern auch die Einhaltung datenschutzrechtlicher Bestimmungen und die Vermeidung von Interessenkonflikten. In diesem Abschnitt wird beschrieben, wie beim Auftragnehmer spezifische Mechanismen und Verfahren implementiert werden, um eine klare Trennung der Daten nach ihren jeweiligen Verarbeitungszwecken zu gewährleisten:

- Logische Mandantentrennung (softwareseitig)
- Dateiseparierung
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem
- Trennung von Test- und Routineprogrammen
- Trennung von Test- und Produktivdaten
- physikalische Trennung (Systeme/ Datenbanken/ Datenträger) vorhanden
- Mandantenfähigkeit relevanter Anwendungen vorhanden

9. Organisationskontrolle

Das Ziel der Organisationskontrolle besteht darin, die interne Unternehmensstruktur so anzupassen, dass sie den speziellen Anforderungen des Datenschutzes entspricht. Dabei liegt der Fokus darauf, dass die Organisation ihre Abläufe und Prozesse so gestaltet, dass sie den Datenschutzbestimmungen entspricht, anstatt den Datenschutz an die bereits bestehende Struktur anzupassen. Im nachfolgenden

Abschnitt werden die spezifischen Maßnahmen und Strategien erläutert, die der Auftragnehmer implementiert hat, um eine effektive Organisationskontrolle zu gewährleisten:

- Schriftliche Regelungen über Betrieb und Abläufe der Datenverarbeitung
- Mitarbeiter sind verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen
- Urlaubs- und Krankheitsvertretung der Geschäftsführung und des IT-Verantwortlichen
- Schriftliches Programmfreigabeverfahren
- Funktionstrennung im IT-Bereich
- Abstimm- und Kontrollverfahren
- Ermittlung und Festlegung des aktuellen Stands der Technik
- Überprüfung der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen
- Nachweise über regelmäßige Schulungen der Mitarbeiter zum Datenschutz
- Fachkundiger Datenschutzbeauftragter ist schriftlich bestellt (Rechtsanwaltsgesellschaft)
- Datenschutzordnung
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Dokumentation von Datenpannen und Sicherheitsvorfällen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

***Anlage 3* – Genehmigte Subunternehmer**

Unterauftrag-nehmer	**Anschrift**	**Plattform**	**Leistung**	**Angaben zu Datenübermittlung**
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Alle Produkte	Datenverarbeitung auf der Office 365 Plattform Backups	Rechenzentrum in Amsterdam & Dublin
Google Commerce Limited	Gordon House, Barrow Street 4, Dublin 4, Ireland	MEA-Frontend MEA-Backend Polario	Hosting der Anwendung und des Backends bei Nutzung des Cloud Deployments Backups Hosting des Tracking Tools	Rechenzentrum in Frankfurt
all-inkl.com	Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland	MEA-Frontend MEA-Backend Registr-Frontend Frontende der Pre-Event-Page Web-Module	Deployment von Schnittstellen Hosting Formulare Tool	Rechenzentrum in Dresden
Freshworks GmbH	Alte Jakobstraße 85/86, 10179 Berlin, Deutschland	Alle Produkte	Ticketsystem und IT Helpdesk	Rechenzentrum in Frankfurt
3Q GmbH	Kurfürstendamm 102, 10711 Berlin, Deutschland	MEA Polario	Streaming und Hosting von Mediendaten (Aufzeichnungen)	Rechenzentrum innerhalb der EU
Sendbird	400 1st Ave,San Mateo, CA 94401, USA	Polario	Chat und Textnachrichten sowie Kommentare	Rechenzentrum in Frankfurt
MongoDB	1633 Broadway, 38th Floor, New York, NY 10019, USA	Polario	Hosting von Datenbanken	Rechenzentrum in Frankfurt
SINCH Mailjet	Office Location, Paris HQ,43 rue de Dunkerque, 75010 Paris, France	MEA Polario	E-Mail Services	Rechenzentrum innerhalb der EU
Slido	Sli.do s.r.o.,Vajnorská 100/A, 831 04 Bratislava, Slovakia	MEA Polario	Umfragen	Rechenzentrum innerhalb der EU

***Anlage 4* – Weisungsberechtigte Personen**

Weisungsberechtigte Personen/Abteilung des Auftraggebers:

Fortlaufende Nummer:	1
Name:	
Organisationseinheit:	
Kontaktdaten für die Kommunikation:	

Fortlaufende Nummer:	2
Name:	
Organisationseinheit:	
Kontaktdaten für die Kommunikation:	

Weisungsberechtigte Abteilungen des Auftragnehmers:

Fortlaufende Nummer:	1
Abteilung:	Projekt Manager im **Customer Support**
Name Teamleitung:	**Nicole Sauter**
Kontaktdaten für die Kommunikation:	**support@plazz.ag**