Vertrag bei Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO zwischen

– Auftraggeber –

und

– Auftragnehmer –
Actionbound GmbH
Bahnhofstraße 82
82383 Hohenpeißenberg
Deutschland

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Nr.	Zweck	Betroffenengruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist
1	Accounterstellung	a) Kunden b) Bound-Ersteller c) Bound-Spieler	E-Mail-Adresse, Nutzername (oder Pseudonym)	Finanzbuchhaltung, Vertrieb, Support	nicht vorgesehen	bei Kündigung des Accounts, bei Widerruf
2	Nutzung der Erstellersoftware, Bound-Erstellung	Bound-Ersteller	Logindaten, ggf. Mediadaten, freiwillig vom Ersteller eingegebene Daten von Nutzern oder Erstellern	Support, Bound-Ersteller, Bound-Spieler	nicht vorgesehen	bei Kündigung des Accounts, bei Widerruf
3	Nutzung der App und Bounds	a) Bound-Ersteller b) Bound-Spieler	E-Mail-Adresse (freiwillig), Name (oder Pseudonym), vom Bound-Ersteller zur Verfügung gestellte Daten, Medien (Bild, Ton), Geodaten	Support, Bound-Ersteller, Bound-Spieler	nicht vorgesehen	bei Kündigung des Accounts, bei Widerruf
4	Auswertung und Bereitstellung der Spielergebnisse	Bound-Spieler	E-Mail-Adresse (freiwillig), Name (oder Pseudonym),	Support, Bound-Ersteller, Bound-Spieler	nicht vorgesehen	bei Kündigung des Accounts, bei Widerruf

			vom Bound-Spieler eingegebene Daten, Medien (Bild, Ton)			
5	Logfiles zur Systemüberwachung, Vorbeugung von Missbrauch	Websitebesucher, Appbenutzer	IP-Adresse	Administration	nicht vorgesehen	1 Woche

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art.4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, es sei denn, es liegt ein vorgesehener Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der DS-GVO (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der

Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Artt. 33 bis 36 DS-GVO genannten Pflichten und bei sonstigen Anfragen von Aufsichtsbehörden.
(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen, dies ist bis auf Weiteres Herr Simon Zwick.
(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
(11) Übermittlungen der Daten in Drittländer sind nicht vorgesehen und werden, soweit technisch möglich, ausgeschlossen.
(12) Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DS-GVO.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 10 entsprechend.
(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Auftraggeber und Auftragnehmer verständigen sich darauf, dass der Nachweis durch folgende Unterlagen erbracht wird: Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO, Verzeichnis der Verarbeitungstätigkeiten (Auszug).

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.
(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz
Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Datum _____

Unterschriften

_____

Simon Zwick

Anhang
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO
Genehmigte Subunternehmer

Dokumentation der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes bei Actionbound

Actionbound GmbH, nachfolgend “Actionbound” genannt.

Zutrittskontrolle

Verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben.

Für die Räumlichkeiten der Datenverarbeitungsanlagen muss zwischen Rechenzentrum und Büroräumen unterschieden werden.

Rechenzentrum

Die Rechenzentren werden in Deutschland von Hetzner Online GmbH, 1&1 Internet SE und Amazon Web Services, Inc. betrieben. Amazon Web Services, Inc. hat vertraglich zugesichert, alle Daten ausschließlich in Rechenzentrum im Großraum Frankfurt/Main zu verarbeiten. Mit den Rechenzentrumsbetreibern besteht jeweils eine Vereinbarung zur Auftragsdatenverarbeitung.
Der Zugang zum Rechenzentrum wird durch den Rechenzentrumsbetreiber kontrolliert. Der übliche, hohe Industriestandard zur Zutrittskontrolle wurde Actionbound vertraglich zugesichert und bei der Auswahl der Dienste berücksichtigt. Die Dokumentation kann auf Nachfrage von Actionbound versandt werden.

Büroräume

Büroräume sind die Räumlichkeiten am Firmensitz von Actionbound in Hohenpeißenberg und im Büro Berlin. Zum anderen ist es einzelnen Mitarbeitern, die sich als besonders vertrauenswürdig erwiesen haben, auch gestattet, von anderen Orten aus zu arbeiten (z. B. auf einer Dienstreise). Mitarbeitern mit Leitungsfunktion, die sich als besonders zuverlässig erwiesen haben, wird im Einzelfall gestattet, aus einem abschließbaren häuslichen Arbeitszimmer zu arbeiten. Alle Mitarbeiter sind schriftlich zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung verpflichtet. Es wird durch entsprechende Weisungen an alle Mitarbeiter sichergestellt, dass sich in Büroräumen grundsätzlich

keine unverschlüsselten Kunden- oder Verwaltungsdaten befinden und keine unverschlüsselten Kunden- oder Verwaltungsdaten aus den Büroräumen mitgenommen werden.

Daher ist für die Büroräume keine spezielle Zutrittskontrolle erforderlich. Die Sicherungsmechanismen entsprechen denen normaler gewerblich genutzter Räumlichkeiten, d. h. Türschloss mit protokollierter Schlüsselvergabe, Jalousien.

Zugangskontrolle

Verhindern, dass Unbefugte Datenverarbeitungsanlagen nutzen können.

Rechenzentren

Auf den Servern in den Rechenzentren sind die Kunden- und Verwaltungsdaten zentral gespeichert. Die Zugangskontrolle zu diesen Servern ist deshalb von besonderer Bedeutung.

Die Server im Rechenzentrum verfügen zur Administration über entsprechende Benutzerkonten. Die Administration der Server erfolgt über das Internet über ein verschlüsseltes Protokoll mit Zugang über 4096 bit RSA Schlüsseln. Diese Schlüssel sind nur der Geschäftsführung bekannt und werden regelmäßig geändert.

Rechner der Mitarbeiter

Der Zugang zu den Rechnern der Mitarbeiter wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter ein eigenes Benutzerkonto sowohl für den lokalen Rechner, als auch für die Verwaltungssoftware, mit deren Hilfe auf die Kunden- und Verwaltungsdaten im Rahmen des Supports kontrolliert zugegriffen werden kann (s. Zugriffskontrolle). Die Mitarbeiter sind dazu verpflichtet, Passwörter laut Empfehlung des Bundesamts für Sicherheit in der Informationstechnik zu benutzen. Die Übertragung zwischen den Rechenzentren zu den Rechnern der Mitarbeiter ist verschlüsselt.

Zugriffskontrolle

Gewährleisten, dass nur Berechtigte auf Daten zugreifen können und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können.

Der Zugriff auf Kundendaten ist nur geschulten Mitarbeitern von Verkauf, Buchhaltung und Support, sowie der Geschäftsführung möglich. Dies wird durch Vergabe von Berechtigungen durch die Geschäftsführung an die Mitarbeiter sichergestellt.

Actionbound hat mit jedem Mitarbeiter eine schriftliche Vereinbarung über die sichergestellt wird, dass Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Weitergabekontrolle

Gewährleisten, dass Daten bei der elektronischen Übertragung/Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die Weitergabekontrolle wird bei Actionbound durch die Speicherorte der Kunden- und Verwaltungsdaten in den Rechenzentren und die restriktive Zutritts- und Zugangskontrolle zu diesen Speicherorten sichergestellt. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von im Rechenzentrum gespeicherten Daten durch den Rechenzentrumsbetreiber ist vertraglich ausgeschlossen. Zur Übertragung sind die Daten – wie oben unter Zugangskontrolle angegeben – verschlüsselt.

Eingabekontrolle

Gewährleisten, dass nachträglich überprüft werden kann, ob und wer Daten verändert oder entfernt hat.

Um die Eingabekontrolle sicherzustellen, werden bei Actionbound die Eingaben, die die Mitarbeiter in der Kundenverwaltung durchführen, protokolliert. Mit dieser Protokolldatei kann jederzeit nachvollzogen werden, welche Eingaben oder Änderungen durch welchen Mitarbeiter vorgenommen wurden. Duplikate der Protokolldatei werden georedundant gesichert.

Auftragskontrolle

Gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können.

Mit allen Datenverarbeitern besteht eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung über die sichergestellt ist, dass die Daten nur entsprechend den Weisungen von Actionbound verarbeitet werden. Eine Nutzung oder Weitergabe der Daten durch Mitarbeiter der Datenverarbeiter ist vertraglich ausgeschlossen.

Verfügbarkeitskontrolle

Gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Verfügbarkeit der Daten wird durch ein mehrstufiges Sicherungskonzept gewährleistet. Die erste Stufe bilden die Server selbst mit ihren gespiegelten Festplatten (RAID). Der Ausfall einer Festplatte hat damit keinen Datenverlust zur Folge. Defekte Festplatten können im laufenden Betrieb ausgetauscht werden (Hot-Plug). Der Status des RAID-Systems wird regelmäßig überwacht und bei einer Störung wird der Rechenzentrumsbetreiber mit dem Austausch der defekten Festplatte beauftragt.

Als zweite Sicherungsstufe werden die Daten parallel auf einem zweiten Rechner im Rechenzentrum vorgehalten, um bei einem Ausfall des Primärsystems unverzüglich Zugang zu erhalten.

Als dritte Sicherungsstufe werden die Daten täglich komprimiert und nach dem etablierten Stand der Technik verschlüsselt in ein separates, örtlich getrenntes Backup-Rechenzentrum übertragen.

Im Rechenzentrum bieten vollklimatisierte Sicherheitsräume Schutz vor Gas, Wasser und Feuer. Der zusätzliche Speicherort im Backup-Rechenzentrum sichert darüber hinaus auch größte anzunehmende Unfälle ab, wie z.B. einen Flugzeugabsturz in das erste Rechenzentrum.

Getrennte Verarbeitung

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Daten, die zu unterschiedlichen Zwecken erhoben werden (z. B. Lizenzen, Bound-Erstellung, Bound-Ergebnisse), werden in unterschiedlichen Datenbanksammlungen gespeichert.
Die Test-, Qualitätssicherungs- und Produktionssysteme laufen auf unterschiedlichen Instanzen mit komplett getrennten Datenbanken. Die Datenbanken sind logisch von der Applikationsschicht getrennt. Die Synchronität der Datenbanken wird durch Replikation sichergestellt.

Genehmigte Subunternehmer

Die Actionbound GmbH beauftragt die folgenden Unterauftragsverarbeiter unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 – 4 EU-DSGVO.

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland
(Rechenzentren Nürnberg und Falkenstein)

1&1 IONOS SE
Elgendorfer Str. 57
56410 Montabaur
Deutschland
(Rechenzentrum Karlsruhe)

AWS EMEA SARL
38 avenue John F. Kennedy,
L-1855 Luxembourg
(Rechenzentrum Frankfurt am Main)

Stand: 29.03.2023