Vereinbarung zur Auftragsverarbeitung (AVV) gemäß Art. 28 ABS. 3 DS-GVO

zwischen dem Lizenznehmer (Nutzer der teambits Plattform) bzw. Auftraggeber von Dienstleistungen im Zusammenhang mit der teambits Plattform im Sinne der Allgemeinen Geschäftsbedingungen der teambits GmbH in ihrer jeweils aktuellen Fassung (hiernach „AGB“) als Verantwortlicher (hier bezeichnet als „Auftraggeber“) und teambits GmbH, Robert-Bosch-Str. 7, 64293 Darmstadt als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“).

Stand: 11. Juli 2023

Präambel

(1) Der Auftraggeber beauftragt den Auftragnehmer mit den in § 3 genannten Leistungen.

(2) Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für den Auftraggeber ist Der Landesbeauftragte für den Datenschutz in dem Bundesland, in dem der Auftraggeber seinen Sitz hat.

(2) Zuständige Aufsichtsbehörde für den Auftragnehmer ist der Hessische Beauftragte für Datenschutz und Informationsfreiheit.

(3) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich „digital unterstützter Partizipation, Moderation, Abstimmungen und Wahlen“ auf Grundlage des im Sinne der AGB zustande kommenden Lizenz- und Dienstleistungsvertrags („Hauptvertrag“). Dabei erhält der Auftragnehmer möglicherweise Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und gegebenenfalls der dazugehörigen Leistungsbeschreibung). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

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

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

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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.

(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. Die weisungsberechtigten Personen ergeben sich aus Anlage 5. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(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.

(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

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

§ 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 an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen 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. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der

- Pseudonymisierung und Verschlüsselung
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- Bewertung der Wirksamkeit

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vorherige Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als externer Datenschutzbeauftragter bestellt: dapex - data protection experts. SH Beratungs & Beteiligung UG (haftungsbeschränkt) Tim Steininger, Zertifizierter externer Datenschutzbeauftragter (DSC), Heinrich-Hertz-Str. 2A, 64295 Darmstadt, Tel. 0800–80 500 88, dsb@dapex.eu).

Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. 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 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser 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 auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den 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 Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest die in Art. 33 Abs. 3 DS-GVO enthaltenen Informationen:

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) 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 als „Verantwortlichem“ im Sin-ne der DS-GVO liegen.

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

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen 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.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(9) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO zu unterstützen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig während der Dauer des Hauptvertrags von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen. 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 nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem unmittelbaren 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 erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis 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) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Subunternehmers zugestimmt hat. Die Zustimmung gilt als erfolgt, sofern der Auftraggeber der Unterbeauftragung nicht binnen 30 Tagen, nachdem der Auftragnehmer diesen von der weiteren Unterbeauftragung in Kenntnis gesetzt hat, widerspricht. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern

diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(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 zustimmungspflichtige Subunternehmerverhältnisse 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

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

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber, informiert den Auftraggeber unverzüglich und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer allein der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

(3) Im Übrigen wird bezüglich der Haftung für Datenschutzverstöße auf Art. 82 DS-GVO verwiesen, der uneingeschränkt gilt, wenn und soweit nicht im Rahmen dieser Vereinbarung explizit etwas Anderweitiges geregelt ist.

§ 12 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer zunächst eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, 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. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757–1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

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

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

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

Anlagenverzeichnis

Anlage 1 – Beschreibung der personenbezogenen Daten / Datenkategorien

Anlage 2 – Beschreibung der Betroffenen / Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers (TOMs)

Anlage 4 – Genehmigte Subunternehmer

Anlage 5 – Weisungsberechtigte Personen

Anlage 1 – Beschreibung der personenbezogenen Daten / Datenkategorien

Alle Daten, die der Auftraggeber in seinem teambits Account hinterlegt oder mittels seines teambits Accounts erhebt.

Unter anderem können folgende Datenarten Gegenstand der Verarbeitung sein: Name, E-Mail-Adressen, Telefonnummern, Adressen, Geburtsdatum, Anrede/ Geschlecht, Betriebszugehörigkeit/ Beschäftigungen, Mitgliedschaften/ Mitgliedsnummern, sämtliche Daten die im Rahmen der Partizipation durch Nutzer der Plattform eingegeben oder abgefragt werden, z.B. auch ausgedrückte politischen Meinungen, Antworten auf Fragestellungen des Auftraggebers bei Umfragen oder Abstimmungsverhalten bei durchgeführten Abstimmungen/Wahlen.

Anlage 2 – Beschreibung der Betroffenen / Betroffenengruppen

Kreis der von der Datenverarbeitung betroffenen Personen: Lieferanten, Kunden, Endkunden, Mitarbeiter, Mitglieder, Veranstaltungsteilnehmer, Referenten.

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers (TOMs) – (gemäß Art. 32 DS-GVO)

Organisationskontrolle

- Alle System- und Infrastrukturkomponenten verwenden einzigartige sichere Kennwörter. Es gibt keine Standardzugänge.
- Mindestens nach jedem Ausscheiden eines MA erfolgt eine Überprüfung der Zugangsberechtigungen.
- Es existiert ein geregeltes Vergabeverfahren für Zugangsberechtigungen und deren Entziehung.

Zugangskontrolle

- Der physische Zutritt zu den Büroräumen ist 24h am Tag grundsätzlich verschlossen.
- Es existiert ein elektronisches Zutrittskontrollsystem mit personalisierten Transpondern.
- Serverräume im Büro sind zusätzlich verschlossen.
- Serverracks sind verschlossen. Einen Schlüssel hat nur ein sehr kleiner, notwendiger Personenkreis.
- Kundendaten werden Rechenzentren von Subdienstleistern mit Standort in Deutschland verarbeitet.

Datenträgerkontrolle

- Alle beweglichen Datenträger sind vollverschlüsselt.
- Die Vernichtung von Datenträgern erfolgt immer kontrolliert.
- Aus Sicherheitsgründen werden Daten grundsätzlich nicht mittels externer physischer Datenträger transportiert.
- Es existieren dokumentierte Regeln für die sichere Lagerung von physikalischen Datenträgern.

Speicherkontrolle

- Für alle Systeme existieren adäquate Kennwortrichtlinien, individuelle Benutzeraccounts, sowie geeignete Rollenkonzepte.

Benutzerkontrolle

- Überwachung und Protokollierung von administrativem Systemzugang und Konfigurationsänderungen.
- Für alle Systeme zur Verarbeitung von personenbezogenen Daten existieren individuelle Nutzerprofile und Rollenkonzepte.
- Passwort-Hashing (inkl. Salt) wird nach aktuellem Stand der Technik eingesetzt.

Zugriffskontrolle

- Der Zugang zum Intranet ist durch individuelle Benutzeraccounts gesichert (W-LAN Verschlüsselung mit WPA2 Enterprise, Fernzugang via VPN nach aktuellem Stand der Technik).
- Nach Möglichkeit erfolgt eine Trennung von Anwendungs- und Administrationszugängen.
- Es existiert ein Verbot/Unterbindung von nicht autorisierten Software-Installationen.
- Sicherheits-Patches für Produktivsysteme werden unverzüglich eingespielt.
- Nutzung eines Aktenvernichters mit ausreichender Sicherheitsstufe (vgl. DIN 66399).
- Protokollierung von benutzerrelevanten Aktivitäten (Anmeldung, Abmeldung, Zugriffe, Zugriff-Verweigerung, etc.)

- Automatische Sitzungsbeendigung bei Inaktivität ist auf allen Firmenrechnern voreingestellt.
- Es existiert ein vorgeschriebener Prozess inklusive der benötigten Infrastruktur zur verschlüsselten Passwortspeicherung und -Verwaltung.

Übertragungskontrolle

- Verschlüsselung von Daten während der Übertragung nach aktuellem Stand der Technik (TLS 1.2, TLS 1.3, AES 256).
- Dynamische Zugangsbeschränkungen für bestimmte IP-Adressbereiche.
- Schutz der Infrastruktur durch Firewalls.
- Schutz der Infrastruktur durch Intrusion Detection-Systeme.
- Datenzugriffe und Übermittlungen werden protokolliert.
- Mitarbeiter werden regelmäßig auf Richtlinien/Vorgaben für die Datenübertragung und -weitergabe sowie das Erkennen und den Umgang mit Phishing-Attacken geschult (Präventionsmanagement)

Eingabekontrolle

- Eingesetzte Rollenkonzepte verhindern unautorisierte Eingaben.
- Eingaben/ Datenmanipulationen werden protokolliert.

Transportkontrolle

- Auf den Transport von physischen Datenträgern wird wenn möglich verzichtet.
- Wenn physische Datenträger unausweichlich sind, werden diese immer lückenlos verschlüsselt.

Wiederherstellbarkeit

- Für Kundendaten in Produktivsystemen werden regelmäßig, automatische Sicherungskopien erstellt und in unabhängige, externe Systeme übertragen.
- Die Integrität und Wiederherstellbarkeit der Sicherungskopien wird regelmäßig überprüft.
- Es existiert ein detailliertes Desaster-Recovery Konzept zur schnellen Wiederherstellung aus Sicherungskopien nach einem Zwischenfall.

Zuverlässigkeit

- Die Verfügbarkeit und der Zustand von Produktivsystemen werden durch dedizierte Dienste live überwacht. Bei Auffälligkeiten werden die zuständigen Mitarbeiter sofort und automatisch informiert.
- Die Zuverlässigkeit der für die teambits Plattform relevanten Infrastruktur wird unter anderem auch durch Maßnahmen der in Anlage 4 gelisteten Subunternehmer durch typische Maßnahmen wie redundante Anbindung, redundante Stromversorgung, Hardwareredundanzen, Überwachung der Lebensdauer von Datenträgern, etc. gewährleistet.

Datenintegrität

- Systeme werden in Testumgebungen auf zuverlässige Datenverarbeitung getestet.
- Regelmäßige Datensicherungen sowie ein detailliertes Desaster-Recovery Konzept ermöglichen eine vollständige Wiederherstellung, sollten Daten durch eine Fehlfunktion beschädigt werden.

Auftragskontrolle

- Eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO geschieht nur mit entsprechender Weisung des Auftraggebers.
- Mitarbeitern ist es untersagt, Daten in unbefugter Weise zu kopieren oder zu übertragen.
- Die Auswahl von Subunternehmern geschieht unter Berücksichtigung von Qualitätskriterien, darunter unter anderem entsprechende Zertifizierungen.
- Die Zusammenarbeit mit Subunternehmern erfolgt nur nach sorgfältiger Prüfung durch unseren Datenschutzbeauftragten.

Verfügbarkeitskontrolle

- Die Aufbewahrung von Sicherungskopien geschieht in unabhängigen Systemen.
- Es existiert ein verschriftlichtes Backup-Konzept.
- Notfallpläne sind vorhanden (z.B. für Server-Ausfälle).
- Automatische Systemüberwachung und Benachrichtigung der Administratoren bei Anomalien oder Auffälligkeiten.

Trennungsgebot

- Trennung von Entwicklungs-, Test- und Produktivsystemen.
- Keine Nutzung von Produktivdaten zu Testzwecken, außer dies ist zur Reproduktion von spezifischen Zuständen notwendig und mit den betroffenen Kunden abgesprochen.
- Kundendaten werden nur von den jeweils zuständigen Mitarbeitern verarbeitet. Ein Zugriff durch Mitarbeiter ohne entsprechende Zuständigkeit wird nach Möglichkeit durch Einschränkungen der Zugriffsrechte verhindert.
- Kundendaten werden durch ein softwareseitiges Mandantenkonzept getrennt und vor unberechtigten Zugriffen durch andere Nutzer geschützt.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Alle Mitarbeiter werden regelmäßig zu Themen des Datenschutzes geschult.
- Alle Mitarbeiter, die im Rahmen ihrer Tätigkeit mit der Verarbeitung personenbezogener Daten in Berührung kommen sind auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Dies geschieht bei der Einstellung neuer Mitarbeiter mittels einer vertraglichen Verpflichtungserklärung, die jeder Mitarbeiter abzugeben hat.
- teambits pflegt ein Verzeichnis von Verarbeitungstätigkeiten im Sinne des Art. 30 Absatz 1 und 2 DS-GVO. Dieses Verarbeitungsverzeichnis ist nicht öffentlich.
- Die technisch-organisatorischen Maßnahmen werden regelmäßig reevaluiert und bei Bedarf angepasst.

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

all-inkl.com	ALL.INKL.COM - Neue Medien Münnich, Hauptstr. 68, D-02742 Friedersdorf	teambits-Webseite, E-Mails
Hetzner Online GmbH	Industriestraße 25, D-91710 Gunzenhausen	Hosting der teambits Plattform sowie operativer Anwendungen wie Chat-, Support-, CRM-Systeme, etc.
netcup GmbH	Daimlerstraße 25, D-76185 Karlsruhe	Hosting der teambits Plattform sowie operativer Anwendungen wie Chat-, Support-, CRM-Systeme, etc.
Amazon Web Services Inc. (Hosting-Location: Frankfurt (Main), Deutschland)	410 Terry Avenue North, Seattle, WA 98109, United States	Versand von E-Mails und Push-Benachrichtigungen
mes.mo GmbH	Herdweg 16, D-73035 Göppingen	SMS-Versand über die Plattform Any-sms
Celonis, Inc.	One World Trade Center 87th Floor, New York, NY 10006, United States	Nutzung der Plattform make.com zur Automatisierung von Geschäftsprozessen und Datenflüssen, unter anderem Nutzerregistrierungen, Supportanfragen und Abrechnungen
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107 USA	Content Delivery Network, Domain Name Server, DDoS-Schutz, Reverse Proxy
sipgate GmbH	Gladbacher Str. 74, D-40219 Düsseldorf	Telefonanlage inkl. Adressbuch
MWC - Mobile World Communications GmbH	Kavalierstr. 9, D-13187 Berlin	Virtuelle Telefonzentrale
troii Software GmbH	Industriezeile 54, 5280 Braunau am Inn, Österreich	Arbeits- und Projektzeiterfassung mittels der Plattform timr.com
GGS Management GmbH	Ernst-Augustin Str. 12 12489 Berlin	Teilnehmersupport (nur nach gesonderter Beauftragung durch den Auftraggeber)
Mail Boxes Etc. Center 0069	Groß-Gerauer Weg 57, D-64295 Darmstadt	Erstellung und Versand von personalisierten Druckprodukten und Mailings (nur nach gesonderter Beauftragung durch den Auftraggeber)

Anlage 5 – Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers sind die gesetzlichen Vertreter des Auftraggebers sowie die von diesen schriftlich benannten Personen.

Weisungsempfänger beim Auftragnehmer sind die gesetzlichen Vertreter des Auftragnehmers sowie die von diesen schriftlich benannten Personen (z.B. Projektleiter des Hauptvertrags, sofern vorhanden).