klubboard®

DATENSCHUTZ · ART. 28 DS-GVO

Datenschutzvereinbarung zur Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DS-GVO



ZWISCHEN

_____

Name des Vereins / der Organisation

_____

Straße und Hausnummer

_____

PLZ und Ort

als Verantwortlicher (nachfolgend „Auftraggeber“)

UND DER

Digitalagentur PASSGEBER
Kokenmühlenstraße 2
48529 Nordhorn
vertreten durch den Inhaber Alexander Kroeze

als Auftragsverarbeiter (nachfolgend „Auftragnehmer“),

jeder für sich eine „Partei“, zusammen die „Parteien“

Inhalt

1 Begriffsbestimmungen
2 Angabe der zuständigen Datenschutzaufsichtsbehörde
3 Vertragsgegenstand und Laufzeit
4 Art der personenbezogenen Daten sowie Kategorien betroffener Personen
5 Weisungsrecht
6 Schutzmaßnahmen des Auftragnehmers
7 Informationspflichten des Auftragnehmers
8 Kontrollrechte des Auftraggebers
9 Einsatz von Subunternehmern
10 Anfragen und Rechte Betroffener
11 Haftung
12 Außerordentliches Kündigungsrecht
13 Herausgabe und Löschung von Daten
14 Entgelte
15 Schlussbestimmungen
A1 Anlage 1 – Beschreibung der Datenkategorien
A2 Anlage 2 – Kategorien der betroffenen Personen
A3 Anlage 3 – Weisungsberechtigte Personen und Weisungsempfänger
A4 Anlage 4 – Technische und organisatorische Maßnahmen
A5 Anlage 5 – Beauftragte Subunternehmer

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in Ziffer 3 genannten Leistungen beauftragen. 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. Diese Vereinbarung gilt ergänzend zu den Allgemeinen Geschäftsbedingungen von PASSGEBER, abrufbar unter https://passgeber.de/agb/

1 Begriffsbestimmungen

1.1 „Verantwortlicher“ ist gemäß 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.

1.2 „Auftragsverarbeiter“ ist gemäß Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.3 „Personenbezogene Daten“ sind gemäß 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 Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.4 „Besonders schutzbedürftige personenbezogene Daten“ sind:

a) personenbezogene Daten aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (gemäß Art. 9 DS-GVO);

b) personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten und damit zusammenhängenden Sicherungsmaßnahmen (gemäß Art. 10 DS-GVO);

c) genetische Daten (gemäß Art. 4 Abs. 13 DS-GVO);

d) biometrische Daten (gemäß Art. 4 Abs. 14 DS-GVO); und

e) Gesundheitsdaten (gemäß Art. 4 Abs. 15 DS-GVO).

1.5 „Verarbeitung“ ist gemäß 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.

1.6 „Aufsichtsbehörde“ ist gemäß Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedsstaat gemäß Art. 51 DS-GVO eingerichtete und unabhängige Stelle.

2 Angabe der zuständigen Datenschutzaufsichtsbehörde

2.1 Die zuständige Aufsichtsbehörde für den Auftragnehmer ist der Landesbeauftragte für den Datenschutz in Niedersachsen, Prinzenstraße 5, 30159 Hannover.

2.2 Die zuständige Aufsichtsbehörde für den Auftraggeber ergibt sich aus dem Sitz des Auftraggebers.

3 Vertragsgegenstand und Laufzeit

3.1 Der Auftragnehmer erbringt für den Auftraggeber auf Grundlage des abgeschlossenen Vertrags (nachfolgend „Hauptvertrag“) Leistungen im Bereich der digitalen Mitarbeiterverwaltung, -kommunikation und -entwicklung. Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag sowie den dazugehörigen Leistungsbeschreibungen.

3.2 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich.

3.3 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien den folgenden Vertrag. Die Regelungen des vorliegenden Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor.

3.4 Die Bestimmungen dieses Vertrags finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer (einschließlich der Beschäftigten) oder durch den Auftragnehmer beauftragte Subunternehmen mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

3.5 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

3.6 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder einem dokumentierten elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

4 Art der personenbezogenen Daten sowie Kategorien betroffener Personen

4.1 Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Im voreingestellten Standardfunktionsumfang werden grundsätzlich keine besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO verarbeitet. Eine Verarbeitung von Daten nach Art. 9 Abs. 1 DS-GVO ist nicht Teil dieses Vertrags. Bei der Verarbeitung von Daten die der Auftraggeber über individuelle Felder in der Software klubboard® erfasst, obliegt die Verantwortung auf Prüfung der Zulässigkeit der Verarbeitung allein beim Auftraggeber.

4.2 Die Kategorien der betroffenen Personen werden in Anlage 2 dargestellt.

5 Weisungsrecht

5.1 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; 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.

5.2 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; 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.

5.3 Die Weisungen des Auftraggebers werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 3. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

5.4 Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei (3) weitere volle Kalenderjahre aufzubewahren.

5.5 Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt (es wird auf Ziffer 14.3 hingewiesen).

5.6 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.

6 Schutzmaßnahmen des Auftragnehmers

6.1 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.

6.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO getroffen hat. Der Auftragnehmer trifft insbesondere die in Anlage 4 aufgeführten Maßnahmen der:

a. Zutrittskontrolle;
b. Zugangskontrolle;
c. Zugriffskontrolle;
d. Trennungskontrolle;
e. Weitergabekontrolle;
f. Eingabekontrolle;
g. Verfügbarkeitskontrolle; und
h. Auftragskontrolle.

6.3 Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

6.4 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 Vertrags betraut werden (nachfolgend „Mitarbeiter“), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit gemäß 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 Vertrags oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

6.5 Beim Auftragnehmer ist ein Datenschutzbeauftragter oder ein Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DS-GVO nicht bestellt werden muss) eingesetzt. Der Ansprechpartner für den Datenschutz kann unter datenschutz@klubboard.de erreicht werden.

7 Informationspflichten des Auftragnehmers

7.1 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 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; und
- **c.** eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen..

7.2 Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen. 6. Angabe der zuständigen Datenschutzaufsichtsbehörde

7.3 Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Ziffer 7.1 betroffen sind.

7.4 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DS-GVO in angemessener Weise (Art. 28 Abs. 3 lit. f) DS-GVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DS-GVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gemäß Ziffer 5 dieses Vertrags durchführen.

7.5 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 Sinne der DS-GVO liegt.

7.6 Über wesentliche Änderung der Sicherheitsmaßnahmen nach Nr. 7 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

7.7 Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten / Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich durch geeignete Weise mitzuteilen. Grundsätzlich ist eine Aktualisierung auf der Firmenwebsite ausreichend.

7.8 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (gemäß Art. 28 Abs. 3 lit. e) und f) DS-GVO).

8 Kontrollrechte des Auftraggebers

8.1 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 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.

8.2 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.

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.

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

8.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen (es wird auf Ziffer 14.2 hingewiesen).

9 Einsatz von Subunternehmern

9.1 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen 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 vorab schriftlich oder in Textform zugestimmt hat. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund widersprechen. 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) wahrnehmen kann.

9.2 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden (gemäß Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

9.3 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).

9.4 Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

9.5 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, 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

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

10.2 Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner 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.

10.3 Der Auftraggeber hat dem Auftragnehmer die hierdurch entstehenden Kosten zu erstatten (es wird auf Ziffer 14.1 hingewiesen).

11 Haftung

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

11.2 Der Auftragnehmer stellt den Auftraggeber von sämtlichen Ansprüchen frei, wenn er:

a. seinen speziell als Auftragsverarbeiter auferlegten Pflichten aus der DS-GVO nicht nachgekommen ist;

b. die rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen nicht beachtet hat; oder

c. gegen diese Anweisungen gehandelt hat.

11.3 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 Absatz 5 DS-GVO.

11.4 Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrags der des Hauptvertrags.

12 Außerordentliches Kündigungsrecht

12.1 Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

12.2 Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

13 Herausgabe und Löschung von Daten

13.1 Mit Beendigung der Auftragsverarbeitungsvertrags oder des Hauptvertrags hat der Auftragnehmer die übermittelten personenbezogenen Daten gemäß den nachfolgenden Ziffern herauszugeben und zu löschen.

13.2 Der Auftragnehmer ist verpflichtet, die eingebrachten personenbezogenen Daten für einen Zeitraum von 30 Tagen nach Vertragsende aufzubewahren. Der Auftraggeber ist berechtigt, jederzeit bis zum Ablauf dieser Frist in Textform die Herausgabe der personenbezogenen Daten in einem maschinenlesbaren Format oder die Löschung der gespeicherten personenbezogenen Daten zu verlangen oder – sofern möglich – die Daten direkt aus der Software herunterzuladen. Der Auftraggeber ist allein für den rechtzeitigen Export seiner Daten verantwortlich.

13.3 Erteilt der Auftraggeber dem Auftragnehmer eine verbindliche Löschungsweisung in Textform, so ist der Auftragnehmer berechtigt, auch vor Ablauf der Aufbewahrungsfrist gemäß Ziffer 13.2, die Datenlöschung durchzuführen. Hiervon ausgenommen sind lediglich die Daten, hinsichtlich derer der Auftragnehmer gesetzlich zur Aufbewahrung verpflichtet ist. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

13.4 Sollte der Auftraggeber bis zum Ablauf der Frist gemäß Ziffer 25.2 weder die herauszugebenden Daten angefordert noch die Löschung dieser Daten verlangt haben, ist der Auftragnehmer verpflichtet, diese Daten zu löschen.

14 Entgelte

14.1 Soweit der Auftraggeber Unterstützung nach Ziffer 10 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

14.2 Soweit der Auftraggeber nach Ziffer 8 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

14.3 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 der Auftraggeberin an die Auftragnehmerin entstehen, bleiben unberührt.

15 Schlussbestimmungen

15.1 Beide Vertragspartner verpflichten sich gegenseitig zur Wahrung der Vertraulichkeit aller nicht allgemein bekannten Unterlagen und Informationen, welche sich auf die geschäftliche Sphäre des anderen Partners beziehen und ihnen bei Vorbereitung und Durchführung dieses Vertrages zugänglich werden. Diese Pflicht bleibt, solange daran ein berechtigtes Interesse besteht, auch nach der Beendigung des Vertragsverhältnisses aufrecht.

15.2 Soweit nichts anderes vereinbart ist, bedürfen Änderungen und Ergänzungen des Vertrags der Schrift- oder Textform. Dies gilt auch für diese Schriftformklausel.

15.3 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.

15.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist - soweit gesetzlich zulässig - Nordhorn.

Anlagen

Anlage 1 – Beschreibung der Datenkategorien
Anlage 2 – Kategorien der betroffenen Personen
Anlage 3 – Weisungsberechtigte Personen und Weisungsempfänger
Anlage 4 – Technische und organisatorische Maßnahmen
Anlage 5 – Beauftragte Subunternehmer

Ort, Datum:	**Ort, Datum:** Nordhorn, 30.11.2025
	
für den Auftraggeber	für den Auftragnehmer

ANLAGE 1

Beschreibung der Datenkategorien

Folgende Datenkategorien sind regelmäßig Gegenstand der Verarbeitung:

- Personalstammdaten (insb. Name, Anschrift, Geburtsdatum, E-Mail-Adresse und Telefonnummer);
- Vertragsstammdaten (insb. Angaben zum beruflichen Werdegang und zu Weiterbildungen, sowie Arbeitsverträge und Bescheinigungen, die zwischen dem Auftraggeber und seinen Mitarbeitenden geschlossen wurden);
- Abrechnungs- und Leistungsdaten (insb. Bankverbindung, Arbeitszeiten, Abwesenheiten, Krankmeldungen, Urlaubspläne)
- Daten zur Gehaltsabrechnung
- Individuelle Angaben des Auftraggebers

ANLAGE 2

Kategorien der betroffenen Personen

Die Kategorien der betroffenen Personen umfasst regelmäßig:

- Mitarbeiter oder Freiwillige (Ehrenamtliche)
- Ehemalige Mitarbeiter oder Freiwillige (Ehrenamtliche)
- Zukünftige Mitarbeiter, Freiwillige (Ehrenamtliche) oder Bewerber

ANLAGE 3

Weisungsberechtigte Personen und Weisungsempfänger

Weisungsberechtigte Personen des Auftraggebers sind:

Vorname, Name und E-Mail-Adresse

Vorname, Name und E-Mail-Adresse

Weisungsempfänger des Auftragnehmers ist:

Alexander Kroeze, Inhaber der Digitalagentur PASSGEBER

ANLAGE 4

Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen werden durch den Auftragnehmer umgesetzt:

1. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b) DS-GVO

a) Zutrittskontrolle

- Türen grundsätzlich verschlossen
- Sicherheitsschlösser
- personalisiertes Schließsystem auf Transponderbasis
- Besucher können sich nur in Begleitung von Mitarbeitern bewegen

b) Zugangskontrolle

- Der Benutzer- und Administratorenzugriff auf die Software-Lösung klubboard® beruht auf einem rollbasierten Zugriffsberechtigungsmodell
  - Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können
- Bei klubboard® gilt das Prinzip der Minimalberechtigung. Jeder Nutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen
  - Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen
- Einsatz von Firewall-Systemen und Virenscanner
- Alle klubboard Serversysteme speichern Daten ausschließlich auf verschlüsselten Datenträgern ab
- Automatische Sperrmechanismen (Benutzerkonten werden nach 10 fehlgeschlagenen Logins automatisch gesperrt)
- IP Sperre: klubboard® kann standardmäßig nur von deutschen IP-Adressen aufgerufen werden. Diese Sperre kann auf Weisung des Auftraggebers entfernt werden.

c) Zugriffskontrolle

- Zugriffsberechtigung auf die klubboard-Serversysteme ist auf einen kleinen Kreis von Mitarbeitern (Systemadministratoren) beschränkt
- Jeder Zugriff auf klubboard®-Anwendungen durch Systemadministratoren wird mit User-ID, Zeitstempel und Anlass protokolliert und aufbewahrt

d) Trennungskontrolle

- Daten werden pro Auftraggeber in eigener Datenbank mit separatem Datenbank-Login abgelegt

2. Integrität gemäß Art. 32 Abs. 1 lit. b) DS-GVO

a) Weitergabekontrolle

- Datenkommunikation wird verschlüsselt gemäß dem Einsatz von VPN-Technologie und TLS
- Serverseitig besteht ein ständig aktualisiertes Firewall- und Virenschutzkonzept
- Endgeräte werden marktüblich gesichert
- E-Mail-Nachrichten werden grundsätzlich verschlüsselt versendet
- eine Speicherung von personenbezogenen Daten auf Datenträgern außerhalb des Rechenzentrums ist nicht vorgesehen

b) Eingabekontrolle

- Jede Eingabe, Änderung und Löschung von Daten sind eindeutig einem User-Login zugeordnet
- Protokollierung von allen administrativen Zugriffen

3. Verfügbarkeit und Belastbarkeit gemäß Art. 32 Abs. 1 lit. b) DS-GVO

a) Verfügbarkeitskontrolle

- Es werden täglich Back-Ups aller klubboard®-Kundendaten erstellt
- Daten sind redundant gesichert
- Die Systeme werden fortlaufend überwacht
- Server befinden sich in sicheren, geschützten, trockenen und klimatisierten Umgebungen
- Regelmäßige Belastungstest, Stresstest (Penetrationstest)
- Erkennen von Systembelastungen
- Regelmäßiges Updaten der IT-Systeme

b) Rasche Wiederherstellbarkeit (gemäß Art. 32 Abs. 1 lit. c) DS-GVO)

- Back-Ups werden regelmäßig auf Wiedereinspielbarkeit geprüft
- Mehrfach-redundante Auslegung von Serversystemen

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gemäß Art. 32 Abs. 1 lit. b) DS-GVO

a) Datenschutz-Management

- Mitarbeiter auf Vertraulichkeit / Datengeheimnis verpflichtet
- Inhaber der Digitalagentur ist sensibilisiert für das Thema Datenschutz

b) Incident-Response-Management für die Software-Lösung klubboard®

c) Datenschutzfreundliche Voreinstellungen (gemäß Art. 25 Abs. 2 DS-GVO)

d) Auftragskontrolle

- Keine Auftragsverarbeitung ohne entsprechende Weisung des Auftraggebers
- Klare, eindeutige Weisungen
- Verhinderung von Zugriffen unbefugter Dritter auf die Daten
- Verbot, Daten in unzulässiger Weise zu kopieren
- Nachkontrollen

ANLAGE 5

Beauftragte Subunternehmer

Folgende Subunternehmer werden durch den Auftragnehmer zur Datenverarbeitung beauftragt:

Name	Funktion	Anschrift
Michael Plas IT-Dienstleistungen	Development	Hasenstrasse 23 | 48465 Schüttorf | Deutschland
Sebil Satici	Development	Edelweißweg 5 | 22523 Hamburg | Deutschland
Neue Medien Münnich | ALL-INKL.COM	Hosting & Domains	Hauptstrasse 68 | 02742 Friedersdorf | Deutschland
Google Ireland Limited	Google Cloud – G Suite G	Gordon House, Barrow Street | Dublin 4 | Ireland
MOCO / hundertzehn GmbH	Buchhaltung, Rechnung	In der Weid 15 | 8122 Binz | Schweiz
Zoom Video Communications Inc.	Videotelefonie	55 Almaden Blvd | 6th Floor San Jose | CA 95113
MEETOVO | Lukas & Christof Bludau GbR	Terminvereinbarung	Kasernenstraße 12 | 21073 Hamburg | Deutschland
CleverReach GmbH & Co. KG	Newsletter und Automatisierungen	Schafjückenweg 2 | 26180 Rastede | Deutschland