Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung (DSGVO)

Version 2.2 (01.07.2021)

zwischen

und
Belonio GmbH
Wienburgstraße 207
48159 Münster

im Folgenden:
Auftraggeber

im Folgenden:
Auftragnehmer

§ 1 Einleitung, Geltungsbereich, Definitionen

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien (Belonio GmbH und Auftraggeber) zum Datenschutz, die sich aus der in den AGB-U (Unternehmen) in ihren Einzelheiten beschriebenen Auftragsverarbeitungen ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit den AGB-U in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch diesen beauftragte Subunternehmer mit personenbezogenen Daten des Auftraggebers (Unternehmen) in Berührung kommen können.
In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Textform nach Art. 28 IX DSGVO gemeint.

§ 2 Gegenstand und Dauer der Verarbeitung

Aus den AGB-U ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Datenkategorien	**Zweck der Verarbeitung**	**Kreis der Betroffenen**
Unternehmensdaten (Name, Anschrift)	Tagesgeschäft: Anwendungsentwicklung, Betrieb der Plattform, Marketing und Vertrieb	Auftraggeber
Name/Vorname	Tagesgeschäft: Anwendungsentwicklung, Betrieb der Plattform, Marketing und Vertrieb	Mitarbeiter des Auftraggebers
E-Mail, Telefonnummer	Tagesgeschäft: Anwendungsentwicklung, Betrieb der Plattform, Marketing und Vertrieb	Mitarbeiter des Auftraggebers
Stamm- und Vertragsdaten, Kaufhistorie, Referenznummern	Rechnungslegung, Erstellung von Reports für die Lohnbuchhaltung	Auftraggeber, Mitarbeiter des Auftraggebers

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des zugrunde liegenden Hauptvertrages (AGB-U), sofern sich aus den Bestimmungen dieses Vertrages nicht darüber hinausgehende Verpflichtungen ergeben.
Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in den AGB-U und in der Leistungsbeschreibung konkretisiert sind.
Die Weisungen des Auftraggebers werden anfänglich durch die AGB-U festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

§ 3 Zweck und Rechtsgrundlage der Verarbeitung

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erfüllung des Vertragszwecks zwischen Auftraggeber und Auftragnehmer. Der Vertrag ist nur erfüllbar, wenn die oben genannten personenbezogenen Daten vom Auftraggeber im benefits Portal eingegeben und dort verwendet werden können. Eine Bereitstellung von Benefits kann ohne Verarbeitung dieser Daten nicht erfolgen. Alle Daten, die im Rahmen der technischen und organisatorischen Maßnahmen (siehe Anlage 1) erhoben und gespeichert werden, dienen dem täglichen Geschäftsablauf beim Auftragnehmer.
2) Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist Art. 6 I lit. a) DSGVO. Im Rahmen des Hauptvertrages (AGB-U) hat der Auftraggeber dem Auftragnehmer seine Einwilligung zur Verarbeitung personenbezogener Daten für die oben genannten Zwecke erteilt.
3) Darüber hinaus ist die Verarbeitung personenbezogener Daten für die Erfüllung des Hauptvertrages erforderlich (Art. 6 I lit. b) DSGVO.

§ 4 Pflichten des Auftragnehmers

1) Der Auftragnehmer darf Daten von Betroffenen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.
2) Widerspricht eine Weisung des Auftraggebers dem Sinn und Zweck des Hauptvertrages und würde die Leistung des Auftragnehmers mit Ausführung der Weisung unmöglich oder wesentlich erschwert, so ist der Auftragnehmer nach vorherigem schriftlichem Hinweis zur außerordentlichen Kündigung des gesamten Vertrages berechtigt.
3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
4) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
5) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
6) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten.
8) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der

Verarbeitungstätigkeiten sowie - falls nötig - bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

9) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
10) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenkonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.
11) 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.

§ 5 Technische und organisatorische Maßnahmen

1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen (Technische und organisatorische Maßnahmen, kurz: TOMs) werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum bezüglich des Datenschutzes. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.
2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen und Backups, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
6) Die Verarbeitung von Daten in Privatwohnungen ist dem Auftragnehmer nicht gestattet. Die Verarbeitung von Daten im Auftrag durch Privatgeräte ist ebenfalls unter keinen Umständen gestattet.
7) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

§ 6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

3) Zur Gewährleistung und Kontrolle einer ordnungsgemäßen Löschung nicht mehr benötigter Daten greift der Auftragnehmer auf ein firmeneigenes Löschkonzept zurück.

§ 7 Unterauftragsverhältnisse

1) Die Beauftragung von Subunternehmern ist nur mit Zustimmung in Schrift- oder Textform des Auftraggebers im Einzelfall zugelassen.
2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.
3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.
4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.
5) Eine weitere Subbeauftragung durch den Subunternehmer ist zulässig, soweit die Rechte und Pflichten dieser Vereinbarung auch an den Sub-Subunternehmer weiter übertragen werden und der Auftraggeber auch hier über entsprechende Kontrollrechte verfügt.
6) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.
7) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.
8) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.
9) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.
10) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür auch der Auftragnehmer gegenüber dem Auftraggeber gemäß einer gesamtschuldnerischen Haftung.
11) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Für diese Subunternehmer gilt die Einwilligung für das Tätigwerden als erteilt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.
12) Die in Anlage 2 genannten Subunternehmer gliedern sich in zwei Kategorien: Subdienstleister für die Bereitstellung und den Betrieb der Anwendung/App, sowie Subdienstleister für die Ausschüttung einzelner Benefits. Da der Auftragnehmer für die Ausschüttung einzelner Benefits mit verschiedenen Projektpartnern zusammenarbeitet, erhalten diese zur Abwicklung der jeweiligen Benefits personenbezogene Daten im Auftrag.
13) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 8 Rechte und Pflichten des Auftraggebers

1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt.

§ 9 Mitteilungspflichten

1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
    a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
    b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
    c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    d) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

§ 10 Weisungen

1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
3) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

§ 11 Beendigung des Auftrags

1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 1.
2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.
3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

§ 12 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

§ 13 Haftung

1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.
3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
4) Nummern 2) und 3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

§ 14 Sonderkündigungsrecht

1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.
3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung - wie in diesem Abschnitt beschrieben - berechtigt.
4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

§ 15 Sonstiges

1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
3) Für Nebenabreden ist die Schriftform erforderlich.
4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
6) Es gilt deutsches Recht.

Anlage 1 zur Auftragsverarbeitung – Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DSGVO

bei

Belonio GmbH, Wienburgstraße 207, 48159 Münster,
vertreten durch Thomas Pry
nachfolgend Belonio genannt

vorgelegt vom ordentlich bestellten Datenschutzbeauftragten

Kontakt:
Belonio GmbH
Datenschutzbeauftragte Anja Wardthuysen
Wienburgstraße 207
48159 Münster
anja@belonio.de

Zutrittskontrolle

- Ein unbefugter Zutritt bzw. Zugang zu DV-Systemen wird verhindert. Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:
    - Türsicherung: Geschäftsräume sind nicht frei zugänglich. Es bestehen elektronische Sicherheitsschlösser und ein elektronisches Transponder-Schließsystem.
    - Schlüssel/Schlüsselvergabe: Gebäudezutrittsschlüssel werden nur an Mitarbeiter/ externe Dienstleister nach sorgfältiger Auswahl, Überprüfung, Verpflichtung und im Rahmen des jeweiligen Auftrags vergeben. Eine entsprechende Protokollierung über vergebene Schlüssel wird durchgeführt.

Zugangskontrolle

- Zugänge: Benutzerrechte werden den Mitarbeitern zugeordnet und dokumentiert. Alle Zugänge sind durch Benutzernamen und Passwort und zusätzlich durch eine 2-Faktor-Authentifizierung gesichert. Es werden aktuelle Verschlüsselungsverfahren verwendet und im Rahmen von Systemupdates regelmäßig aktualisiert. Nach drei Fehleingaben erfolg eine Zugangssperrung und danach keine automatische Freigabe.
- Passwortrichtlinie: Es besteht eine entsprechende Passwortrichtlinie inklusive vorgegebener Passwortlänge und regelmäßigem Passwortwechsel. Eine Doppelanmeldung unter gleichem Namen (Username + Passwort) wird verhindert.
- Nur Belonio hat Zugang zu den Belonio Systemen und kann Personen Zugang gewähren. Wo möglich, wird der Zugang über ein Single-Sign-On System verwaltet.
- Die Anzahl der Administratoren wird auf ein zwingend notwendiges Maß reduziert.

Zugriffskontrolle

- Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen werden durch folgende Maßnahmen verhindert:
    - Zugriff wird nur Belonio Mitarbeitern gewährt, die im Rahmen ihrer Tätigkeit auf entsprechende Daten zugreifen müssen.
    - Speicherkontrolle: Der Zugriff wird durch ein Rollen- und Rechtemanagement sichergestellt, dass von Belonio administriert wird. Rollen und Rechte werden auf die Tätigkeit zugeschnitten.

Transportkontrolle

- Aspekte der Weitergabe personenbezogener Daten sind wie folgt geregelt:
    - Daten, die auf Datenträgern gespeichert werden, werden ausschließlich verschlüsselt auf diesen gesichert.
    - Sender und Empfänger müssen protokolliert sein.
    - Fax-Protokollierung

Übertragungskontrolle

- Daten werden ausschließlich über verschlüsselte Verbindungen übermittelt. Der Datentransfer wird durch Logdateien protokolliert.
- Sender und Empfänger müssen protokolliert sein.

Benutzerkontrolle

- Nur autorisierte Nutzer können mit Benutzername und Passwort zugreifen. Die Rechte können jederzeit zentral entzogen werden.

Eingabekontrolle

- Folgende Maßnahmen gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten im DV-System eingegeben, verändert oder entfernt worden sind:
    - Alle Eingabe- und Änderungsoperationen werden durch Logdateien protokolliert.
    - Der Zugriff wird durch ein Rollen- und Rechtemanagement sichergestellt, dass von Belonio administriert wird. Rollen und Rechte sind auf die jeweiligen Tätigkeiten zugeschnitten.

Verfügbarkeitskontrolle

- Die Daten sind folgendermaßen gegen zufällige Zerstörung oder Verlust geschützt:
    - Belonio erstellt regelmäßig BackUps aller Daten und Protokolle bei AWS in verschiedenen Verzeichnissen und auf verschiedenen Servern.

Trennungskontrolle/ Trennbarkeit der Daten

- Durch folgende Maßnahmen wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene und genutzte Daten bearbeitet werden können:
    - Belonio trennt seine Anwendungen nach fachlichen Rollen. Die Daten der Anwender sind durch logische Schlüssel voneinander separiert. Die Trennung wird durch Kontrollen auf mehreren Ebenen sichergestellt.
    - Zugriffsversuche auf fremde Daten werden protokolliert.

Auftragskontrolle

- Die weisungsgemäße Auftragsverarbeitung wird wie folgt gewährleistet:
    - Jegliche Verarbeitung von Daten erfolgt ausschließlich entsprechend der Weisung des Auftraggebers, die in den AGB-U zwischen Belonio und dem Auftraggeber, sowie im benefits Portal vereinbart wurden.
    - Es erfolgt eine eindeutige Vertragsgestaltung und eine Kontrolle der Vertragsausführung.
    - Die Vernichtung von Daten nach Beendigung des Auftragsverhältnisses unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen wird sichergestellt.

Wiederherstellbarkeit

- Daten und Systeme können jederzeit aus Backups und Spiegelsystemen wiederhergestellt werden. Durch Virtualisierung der Infrastruktur muss keine Hardware wiederherstellbar sein.

Zuverlässigkeit

- Belonio benefits wird ständig überwacht. Bei Fehlern werden Meldungen in mehreren Eskalationsstufen an unterschiedliche Personen gesendet. Das Rechenzentrum und die Dienste-Infrastruktur wird separat vom Betreiber überwacht. Es wird eine Verfügbarkeit von 99,95% garantiert.

Datenintegrität

- Alle personenbezogenen Daten liegen in Datenbanken und Dateisystemen, deren Integrität durch Prüfsummen überwacht wird. Im Falle von Fehlfunktionen werden automatisch Reservesysteme zugeschaltet oder die Daten können manuell mit Backups verglichen und wiederhergestellt werden.

Anlage 2 zur Auftragsverarbeitung – Zugelassene Subdienstleister und Auftragsinhalte

Subdienstleister für die Bereitstellung der Anwendung/APP:

- Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg
  - Datenverarbeitung und Speicherung (auf den AWS-Servern in Frankfurt)
- Atlassian Pty Ltd., Atlassian, Inc., 1098 Harrison Street, San Francisco, CA 94103, USA
  - internes Issuemanagement und Support
- Easybill GmbH, Düsselstraße 21, 41564 Kaarst
  - Rechnungslegung
- Functional Software Inc., Sentry, 132 Hawthorne Street, San Francisco, CA 94107, USA
  - Bug Tracking
- Google Irland Ltd., Gordon House, Barrow Street, Dublin 4
  - firmeninterne Office-Suite (E-Mails, Google Drive etc.)
- HubSpot, Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141 USA
  - Verwaltung von Leads für Marketing und Vertrieb, Chatfunktion auf der Website, Newsletter, CRM, Wissensdatenbank, Kontaktformular & Support-Postfach, Feedback-Umfragen
- Spanning Backup, 1703 W5th St, Suite 650 Austin, TX, 78703
  - Speicherung von Google Office Suite BackUps
- Userlane GmbH, Rosenheimerstraße 143C, 81671 München
  - Unterstützung bei der Systemführung, Bedienungshilfe
- Zoom Videocommunication Inc., 55 Almaden Blvd., 6th Floor, San José, CA
  - Webinar-Software

Subdienstleister (Benefit-Partner) für die Ausschüttung von Benefits (variabel je nach ausgeschütteten Benefits):

- Edenred Deutschland GmbH, Claudius-Keller-Str. 3c, 81669 München
  - Bereitstellung und Aufladung von Ticket Plus Karten by Belonio
- Cadooz GmbH, Osterbekstraße 90b, 22083 Hamburg
  - Bereitstellung und Aufladung von Gutscheinen im Gutscheinpool und MyBen
- Amazon EU S.à r.l. , 38 avenue John F. Kennedy, L-1855 Luxemburg
  - Bereitstellung und Aufladung von amazon.de Gutscheinen
- Zalando Zalando SE, Valeska-Gert-Straße 5, 10243 Berlin
  - Bereitstellung und Aufladung von Zalando Gutscheinen
- Zmyle GmbH, Rekener Straße 39a, 48653 Coesfeld
  - Bereitstellung und Aufladung von regionalen Gutscheinen
- Urban Sports Club GmbH, Alt-Moabit 103, 10559 Berlin
  - Bereitstellung von Urban Sports Fitness Gutscheinen
- MRH-Trowe Benefit & Pensions, Am Ringofen 2, 36304 Alsfeld
  - Bereitstellung von und Beratung zu BAV und Versicherungslösungen
  - Rückmeldung der relevanten Daten zum BAV Vertrag zur Erstellung von Reportings
- Hallesche Krankenversicherung auf Gegenseitigkeit, Rheinsburgstraße 10, 70178 Stuttgart
  - Bereitstellung von und Beratung zu betrieblichen und privaten Krankenversicherungen
- Eurorad Deutschland GmbH, Longerich Str. 2, 50739 Köln
  - Bereitstellung von und Beratung zu Diensträdern
  - Rückmeldung der relevanten Daten zum Leasing Fahrrad zur Erstellung von Reportings
- DD Deutsche Dienstrad GmbH, Sven-Wingquist-Straße 2, 97424 Schweinfurt
  - Bereitstellung von und Beratung zu Diensträdern
  - Rückmeldung der relevanten Daten zum Leasing Fahrrad zur Erstellung von Reportings
- Radelnde Mitarbeiter, Krögerweg 33, 48155 Münster
  - Bereitstellung von und Beratung zu Diensträdern
  - Rückmeldung der relevanten Daten zum Leasing Fahrrad zur Erstellung von Reportings