Vertrag über die Auftragsverarbeitung personenbezogener Daten nach Art. 28 EU Datenschutz-Grundverordnung (DSGVO)

Version 4.1 (01.06.2023)

zwischen

vertreten durch:

im Folgenden:
Auftraggeber

und

Belonio GmbH
Wienburgstraße 207
48159 Münster

vertreten durch:
Marcel Descher,
Thomas Pry

im Folgenden:
Auftragsverarbeiter

§ 1 Einleitung, Geltungsbereich, Definitionen

1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers unter Beachtung der nachfolgenden Bestimmungen. Dieser Vertrag regelt dabei die Rechte und Pflichten von Auftragsverarbeiter und Auftraggeber.

2) Unter dem Begriff „Hauptvertrag“ wird im Folgenden der separat abgeschlossene Vertrag zwischen dem Auftragsverarbeiter und dem Auftraggeber auf Basis der AGB-U des Auftragsverarbeiters oder ein separat geschlossener Nutzungsvertrag verstanden.

3) Dieser Vertrag findet Anwendung auf alle Tätigkeiten, bei denen der Auftragsverarbeiter, Mitarbeiter des Auftragsverarbeiters oder durch ihn beauftragte Unterauftragsverarbeiter personenbezogene Daten des Auftraggebers im Rahmen des Hauptvertrages verarbeiten.

4) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ erfolgen zu haben, ist die Textform nach Art. 28 Abs. 9 DSGVO gemeint.

§ 2 Gegenstand und Dauer der Verarbeitung, Kategorien der Daten und Betroffenen

1) Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenverarbeitung ergeben sich aus dem Hauptvertrag und diesem Vertrag. Im Einzelnen sind folgende Datenarten/ -kategorien regelmäßig Gegenstand der Verarbeitung:
    a) Personalstammdaten (Anrede, Name, Vorname, Geburtsdatum, Personalnummer, E-Mail-Adresse, geschäftliche Telefonnummer der Benefit Piloten)
    b) Vertragsdaten sowie Vertragsabrechnungsdaten (Art der Zuwendung, Datum der Zurverfügungstellung, Intervall, Betrag der jeweiligen Zuwendung, Belegerfassung)

2) Der Gegenstand der Verarbeitung, Kategorien der Daten, Zweck und Umfang der Auftragsverarbeitung sind in Anlage 3 zu diesem Vertrag weiter beschrieben.

3) Die Kategorien der regelmäßig durch die Verarbeitung betroffenen Personen sind aktuelle und ehemalige Mitarbeiter des Auftraggebers.

4) Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrags. Insofern sich aus den Bestimmungen dieses Vertrages darüber hinausgehende Verpflichtungen ergeben, endet dieser Vertrag mit dem Wegfall der über den Hauptvertrag hinaus bestehenden Pflichten.

§ 3 Allgemeine Pflichten des Auftraggebers

1) Der Auftraggeber ist gemäß Art. 4 Nr. 7 DSGVO Verantwortlicher im datenschutzrechtlichen Sinne für die beim Auftragsverarbeiter nach diesem Vertrag verarbeiteten personenbezogenen Daten. Insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter ist er allein verantwortlich. Dies gilt ebenso im Hinblick auf den in § 2 genannten Gegenstand, Umfang, die Art und den Zweck der Datenverarbeitung sowie die Wahrung der Betroffenenrechte.

2) Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich und vollständig, wenn er Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

§ 4 Allgemeine Pflichten des Auftragsverarbeiters

1) Der Auftragsverarbeiter bestellt, soweit gesetzlich vorgeschrieben, 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 Auftragsverarbeiter teilt dem Auftraggeber in Anlage 1 zu diesem Vertrag die Kontaktdaten des / der Datenschutzbeauftragten mit. Im Falle eines Wechsels in der Person werden die neuen Kontaktdaten unverzüglich nach der Bestellung mitgeteilt.

2) Der Auftragsverarbeiter gewährleistet die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29 und 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der für die Auftragsverarbeitung erforderlichen Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragsverarbeiter trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

3) Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers, dem Hauptvertrag und der in diesem Vertrag eingeräumten Befugnisse verarbeiten, es sei denn, dass eine gesetzliche Verpflichtung zur Verarbeitung besteht.

4) Der Auftragsverarbeiter gewährleistet, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und die Rechte der betroffenen Personen gewahrt werden. Insbesondere kontrolliert er dazu regelmäßig die internen Prozesse und technischen und organisatorischen Maßnahmen (TOM).

5) Der Auftragsverarbeiter unterstützt den Auftraggeber im Hinblick auf die Gewährleistung der Melde- und Benachrichtigungspflichten im Fall von Datenschutzverletzungen im Sinne von Art. 33 und 34, sowie Art 35 und 36 DSGVO. Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 5 Informationspflichten des Auftragsverarbeiters

1) Der Auftragsverarbeiter meldet ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten durch den Auftragsverarbeiter, Mitarbeiter des Auftragsverarbeiters oder

durch ihn beauftragte Unterauftragsverarbeiter unverzüglich an den Auftraggeber im Sinne von Art. 33 Abs. 2 DSGVO. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. 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.

2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie grobe Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

3) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich über Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen, insofern keine gesetzliche oder behördliche Verpflichtung für den Auftragsverarbeiter besteht, eine entsprechende Mitteilung zu unterlassen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

§ 6 Kontrollmitwirkung des Auftragsverarbeiters

1) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz, der technischen und organisatorischen Maßnahmen sowie der Pflichten aus diesem Vertrag beim Auftragsverarbeiter in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die eigenen gespeicherten Daten und die Datenverarbeitungsprogramme sowie Vor-Ort-Kontrollen unter Rücksichtnahme auf die berechtigten Interessen des Auftragsverarbeiters, zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragsverarbeiter, soweit erforderlich, Zutritt und Einblick zu ermöglichen. Der Auftragsverarbeiter ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

2) Der Auftragnehmer darf die Zustimmung zu einer Prüfung von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

3) Vor-Ort-Kontrollen beim Auftragsverarbeiter haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden dringlichen Gründen anders angezeigt, finden Vor-Ort-Kontrollen nach angemessener 14-tägiger Vorankündigung zu den üblichen Geschäftszeiten des Auftragsverarbeiters statt. Der Aufwand für anlasslose Vor-Ort-Kontrollen ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt und ist vom Auftraggeber zu tragen.

4) Anlasslose Vor-Ort-Kontrollen können vom Auftragsverarbeiter abgelehnt werden, wenn und solange er geeignete Nachweise, insbesondere zur Umsetzung und Wirksamkeit der TOM, erbringt. Geeignete Nachweise können durch Vorlage aktueller Bescheinigungen, Berichte oder Berichtsauszüge durch unabhängige Sachverständige oder durch entsprechende Zertifikate nach den Grundsätzen der IT-Sicherheit und des Datenschutzes erbracht werden.

§ 7 Pflichten des Auftragsverarbeiters bei Anfragen betroffener Personen

1) Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber im erforderlichen Umfang bei der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen zu unterstützen, soweit die Auftragsverarbeitung betroffen ist.

2) Wendet sich eine betroffene Person mit einer Forderung aus Kapitel III der DSGVO zwecks Wahrnehmung ihrer Betroffenenrechte an den Auftragsverarbeiter, so verweist der Auftragsverarbeiter die betroffene Person an den Auftraggeber, sofern die betroffene Person nach ihren Angaben dem Auftraggeber zugeordnet werden kann.

3) Eine Haftung des Auftragsverarbeiters ist ausgeschlossen, sofern der Auftraggeber allein verschuldet, dass ein Ersuchen einer betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 8 Weisungen durch den Auftraggeber

1) Der Auftraggeber hat im Rahmen dieses Vertrages ein umfassendes Weisungsrecht gegenüber dem Auftragsverarbeiter. Dies gilt insbesondere hinsichtlich der Berichtigung, Löschung, Einschränkung und Weitergabe der Daten sowie über Art, Umfang und Verfahren der Datenverarbeitung. Dieses umfassende Weisungsrecht kann der Auftraggeber durch Einzelweisung konkretisieren.

2) Die Weisungen des Auftraggebers werden anfänglich durch den Hauptvertrag und diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich schriftlich gegenüber dem Auftragsverarbeiter bestätigen.

3) Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange abzulehnen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4) Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Bei solchen Anträgen auf Leistungsänderung teilt der Auftragsverarbeiter dem Auftraggeber mit, wie sie sich auf die vereinbarte Leistung, insbesondere die Möglichkeit der Leistungserbringung und Vergütung, auswirken. Ist die Umsetzung einer Weisung für den Auftragsverarbeiter unzumutbar, so steht dem Auftragsverarbeiter das Recht zu, diese Weisung abzulehnen. Unzumutbar ist die Umsetzung einer Weisung insbesondere, wenn die zu erbringende Leistung mit Ausführung der Weisung unmöglich oder wesentlich erschwert würde. Der Auftraggeber haftet dem Auftragsverarbeiter im Innenverhältnis voll für Schäden, die aus bestätigten Weisungen entstehen und stellt den Auftragsverarbeiter gegen Ansprüche Dritter, die im Zusammenhang mit bestätigten Weisungen des Auftraggebers stehen, auf erstes Anfordern frei.

5) Der Auftraggeber hat dem Auftragsverarbeiter die zu Weisungen ausschließlich befugten Person(en) schriftlich zu benennen. Als schriftlich benannt gelten die im Belonio-Cockpit als Administrator bestimmten natürlichen Personen (Benefit-Piloten). Sofern der Auftraggeber keine weisungsbefugte Person schriftlich benennt, sind ausschließlich vertretungsberechtigte natürliche Personen des Auftraggebers zur Erteilung von Weisungen berechtigt.

§ 9 Sicherheit der Verarbeitung

1) Der Auftragsverarbeiter gewährleistet die Sicherheit der Verarbeitung gemäß Art. 28 Abs. 3 lit. c und 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO durch eine ordnungsgemäße Umsetzung und Einhaltung der in Anlage 1 genauer beschriebenen geeigneten technischen und organisatorischen Maßnahmen (kurz: TOM). Insgesamt handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

2) Die TOM werden durch die Anlage 1 zu diesem Vertrag als verbindlich festgelegt. Sie definieren das vom Auftragsverarbeiter geschuldete Minimum bezüglich der Sicherheit der Verarbeitung.

3) Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Eine Änderung der getroffenen Sicherheitsmaßnahmen ist dem Auftragsverarbeiter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Insoweit ist der Auftragsverarbeiter zur Wirkungsüberprüfung und entsprechender Anpassung bei Fortschritten nach dem Stand der Technik verpflichtet. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.

§ 10 Unterauftragsverarbeiter

1) Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt, gelten nicht als Unterauftragsverarbeitung. Dazu zählen z.B. Nebenleistungen wie Transport, Wartung und Reinigung, die Inanspruchnahme von Telekommunikationsdienstleistungen, Benutzerservice oder Kundenbeziehungsmanagement sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Überprüfungsmaßnahmen zu ergreifen.

2) Der Auftragsverarbeiter wählt sämtliche Unterauftragsverarbeiter sorgfältig aus, insbesondere unter Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Sicherheitsmaßnahmen.

3) Erteilt der Auftragsverarbeiter Aufträge an Unterauftragsverarbeiter, ist er verpflichtet, eine vertragliche Vereinbarung im Sinne des Art. 28 Abs. 2-4 DSGVO mit diesen abzuschließen und seine datenschutzrechtlichen Pflichten aus diesem Vertrag auch auf den Unterauftragsverarbeiter zu übertragen. Insbesondere müssen hinreichende Garantien dafür geboten werden, dass die technischen und organisatorischen Maßnahmen des Unterauftragsverarbeiters die Einhaltung des Schutzniveaus der TOM aus Anlage 1 zu diesem Vertrag sicherstellen.

4) Der Auftragsverarbeiter kann Aufträge an Unterauftragsverarbeiter vergeben, wenn er den Auftraggeber vorab über die Hinzuziehung neuer oder Ersetzung bestehender Unterauftragsverarbeiter schriftlich informiert und der Auftraggeber binnen 4 Wochen keinen Einspruch erhebt. Bei Erteilung des Auftrags durch den Auftraggeber sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und ihr Einsatz mit Abschluss dieses Vertrages vom Auftraggeber genehmigt. Für diese Unterauftragsverarbeiter ist eine Zustimmung des Auftraggebers damit ausdrücklich erteilt. Die niedergelegten sonstigen Pflichten des Auftragsverarbeiters gegenüber den in Anlage 2 genannten Unterauftragsverarbeitern bleiben unberührt.

5) Die Verarbeitung der Daten durch den Auftragsverarbeiter und den vom Auftraggeber genehmigten Unterauftragsverarbeitern findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede sonstige Verarbeitung oder Nutzung außerhalb dieser genannten Gebiete, darf nur erfolgen, wenn die besonderen Voraussetzungen für Datenexporte in Drittländer gemäß Art. 44 ff. DSGVO erfüllt sind, beispielsweise durch die Nutzung der EU-Standardvertragsklauseln. Sind die besonderen Voraussetzungen abhängig von einer Handlung des Auftraggebers (beispielsweise im Falle des Art. 46 Abs. 1, 1. Alt DSGVO), so darf sich der Auftragsverarbeiter nur darauf berufen, wenn diese vom Auftraggeber genehmigt sind.

§ 11 Löschung, Berichtigung und Sperrung von Daten

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

2) Bei Beendigung der Auftragsverarbeitung oder jederzeit auf Verlangen des Auftraggebers hat der Auftragsverarbeiter die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers in einem

maschinenlesbaren Format an den Auftraggeber herauszugeben oder zu löschen. Erteilt der Auftraggeber innerhalb von 30 Tagen nach Ende des Hauptvertrages keine Weisung zur Löschung oder Herausgabe, ist der Auftragsverarbeiter zur Löschung der Daten berechtigt. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3) Der Auftragsverarbeiter ist verpflichtet, die unverzügliche Rückgabe oder Löschung auch bei seinen Unterauftragsverarbeitern herbeizuführen.

4) Zur Gewährleistung und Kontrolle der Einhaltung gesetzlicher Aufbewahrungspflichten und einer ordnungsgemäßen Löschung nicht mehr benötigter Daten greift der Auftragsverarbeiter auf ein firmeneigenes Löschkonzept zurück.

5) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

§ 12 Haftung

1) Der Auftragsverarbeiter hat dem Auftraggeber im Fall der schuldhaften Verletzung datenschutzrechtlicher Gesetze oder Pflichten aus diesem Vertrag den dadurch entstandenen Schaden zu ersetzen, soweit der Schaden nicht durch eine vom Auftraggeber erteilte Weisung entstanden ist.

2) Jegliche Haftungsausschlüsse in diesem Vertrag gelten nicht im Falle von Vorsatz und grober Fahrlässigkeit sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.

3) Insoweit die Haftung nicht durch diesen Vertrag geregelt ist, richtet sie sich nach den Haftungsregelungen des Hauptvertrages.

§ 13 Sonderkündigungsrecht

1) Ein grober Verstoß gegen eine der vorstehenden Regelungen oder die sonstigen datenschutzrechtlichen Bestimmungen berechtigt den Auftraggeber zu einer außerordentlichen Kündigung der Verträge, die der Auftragsverarbeitung zugrunde liegen. Weitere gesetzliche Gründe zur außerordentlichen Kündigung bleiben unberührt.

2) Besteht der Auftraggeber auf die Umsetzung einer für den Auftragsverarbeiter nach § 8 Abs. 4 unzumutbaren Weisung, so ist der Auftragsverarbeiter nach vorherigem schriftlichem Hinweis zur außerordentlichen Kündigung berechtigt. Er kann demnach die Verarbeitung beenden und den Hauptvertrag jederzeit mit sofortiger Wirkung kündigen.

3) Ist die Erbringung der Leistung des Auftragsverarbeiters im Falle eines Einspruchs nach § 10 Abs. 4 ohne Hinzuziehung neuer oder Ersetzung bestehender Unterauftragsverarbeiter für den Auftragsverarbeiter unzumutbar, insbesondere wenn die zu erbringende Leistung ohne die beabsichtige Änderung unmöglich oder wesentlich erschwert würde, ist der Auftragsverarbeiter berechtigt, die Leistung nach vorheriger Ankündigung innerhalb von 8 Wochen einzustellen und den Hauptvertrag fristlos und mit sofortiger Wirkung kündigen.

4) Eine Kündigung nach den Maßgaben des § 13 bedarf stets der Schriftform nach § 126 Abs. 1 und 2 BGB.

§ 14 Schlussbestimmungen

1) Auftraggeber und Auftragsverarbeiter 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) Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Datenhoheit beim Auftraggeber liegt.

3) Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten ausgeschlossen.

4) Auf das Vertragsverhältnis findet deutsches Recht unter Ausschluss des UN-Kaufrechts (CISG) Anwendung.

5) Ausschließlicher Gerichtsstand ist, sofern gesetzlich nicht anders angeordnet, Münster.

6) Änderungen und Ergänzungen dieses Vertrags sind unter dem ausdrücklichen Hinweis darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt, schriftlich abzufassen. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

7) Dieser Vertrag ersetzt mit Ausnahme des Hauptvertrags alle vorherigen oder gleichzeitigen Zusicherungen, Absprachen, Vereinbarungen, Verträge oder Mitteilungen zwischen dem Auftraggeber und dem Auftragsverarbeiter, ob schriftlich oder mündlich in Bezug auf den Gegenstand dieses Vertrags.

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 Auftragsverarbeiter mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DSGVO

bei

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

vorgelegt vom ordentlich bestellten Datenschutzbeauftragten Tobias Kramer

Kontakt:
Belonio GmbH
Datenschutzbeauftragter Tobias Kramer
Wienburgstraße 207
48159 Münster
datenschutz@belonio.de

Grundsätzliche Maßnahmen

- Die Unternehmensleitung hat Verantwortung für Datenschutz und Informationssicherheit übernommen und es besteht ein betriebsinternes Datenschutz-Management.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.
- Die Unternehmensleitung hat einen Datenschutzbeauftragten nach Art. 37 ff. DSGVO bestellt.
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Insofern Datenübermittlungen an Unterauftragsverarbeiter in Drittländern gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments Teil der Auftragsverarbeitung sind, erfolgen diese auf Basis der Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

Zugangskontrolle

Ein unbefugter Zutritt bzw. Zugang zu DV-Systemen wird durch technische und organisatorische Maßnahmen zur Zutrittskontrolle verhindert, 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. Die an Mitarbeiter ausgegebenen Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Zugänge: Benutzerrechte werden den Mitarbeitern zugeordnet und dokumentiert. Alle Zugänge sind durch Benutzernamen und Passwort und nach Möglichkeit zusätzlich durch eine 2-Faktor-Authentifizierung gesichert. Es werden aktuelle Verschlüsselungsverfahren verwendet und im Rahmen von Systemupdates regelmäßig aktualisiert. Nach drei Fehleingaben erfolgt eine Zugangssperrung und danach keine automatische Freigabe.
- Passwortrichtlinie für Mitarbeiter und Nutzer: Es besteht eine entsprechende Passwortrichtlinie zur Verwendung sicherer Passwörter 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.
- Die Anzahl der Administratoren wird auf ein zwingend notwendiges Maß reduziert.
- Verschlüsselung von Festplatten durch Bitlocker, Filevault o.Ä.

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 („Need-to-Know“-Prinzip).
- Speicherkontrolle: Der Zugriff wird durch ein Rollen- und Rechtemanagement sichergestellt, das von Belonio administriert wird. Rollen und Rechte werden auf die Tätigkeit zugeschnitten.

Transport und Übertragungskontrolle

- Daten werden ausschließlich über verschlüsselte Verbindungen übermittelt. Der Datentransfer wird durch Log-Dateien protokolliert.
- Belonio verwendet eine Transportverschlüsselung, wenn Daten über ein unsicheres oder öffentliches Netzwerk (z. B. außerhalb der Virtual Private Cloud) übertragen werden müssen. Die Art der Transportverschlüsselung hängt von der vom Client-System geforderten Verschlüsselung ab. Belonio verwendet HTTPS-Verbindungen mit 256-Bit-SSL-Zertifikaten für die gesamte Kommunikation mit Kunden.
- Daten, die auf Datenträgern gespeichert werden, werden ausschließlich verschlüsselt auf diesen gesichert.
- 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 Log-Dateien protokolliert.
- Der Zugriff wird durch ein Rollen- und Rechtemanagement sichergestellt, das 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 und Regionen innerhalb Deutschlands.
- Es gelten daher die Verfügbarkeitskontrollen von AWS entsprechend.

Trennungskontrolle

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 getrennt. 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 den Weisungen des Auftraggebers, die im Hauptvertrag zwischen Belonio als Auftragsverarbeiter und dem Auftraggeber vereinbart wurden, sowie den späteren Einzelweisungen des Auftraggebers.
- Es erfolgt eine eindeutige Vertragsgestaltung und eine Kontrolle der Vertragsausführung.
- Die Vernichtung von Daten nach Beendigung des Auftragsverhältnisses unter Berücksichtigung der gesetzlichen Aufbewahrungsfristen und vertraglichen Vereinbarung wird sichergestellt.

Wiederherstellbarkeit

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

Zuverlässigkeit

Das Belonio-System wird ständig überwacht. Bei Fehlern werden Meldungen in mehreren Eskalationsstufen an unterschiedliche Personen gesendet. Das Rechenzentrum und die Dienste-Infrastruktur werden 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.

Amazon Web Services EMEA SARL (AWS)

Alle Datenbanken, Anwendungsserver und Netzwerkinfrastrukturen von Belonio werden von Amazon Web Services EMEA SARL (AWS) gehostet. Belonio hat mit AWS zahlreiche TOM vereinbart, insbesondere um einen Datentransfer in ein Drittland sowie unbefugte Zugriffe aufgrund geltender Rechtsvorschriften oder Gepflogenheiten in einem Drittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, verhindern:

- AWS ist mit folgenden industriellen Standardzertifizierungen ausgezeichnet:
    - ISO 27001
    - ISO 27018
    - ISO 27701
    - ISO 9001
    - CSA STAR CCM v4.0
- Ort der Verarbeitung:
    - Belonio nutzt ausschließlich EU-Rechenzentren von AWS. Um sicherzustellen, dass die Daten nicht unbefugt genutzt oder weitergegeben werden können, hat Belonio zudem die Nutzung dieser Dienste vertraglich auf den EU-Raum beschränkt und die Zugriffsmöglichkeiten entsprechend geregelt. Dies gilt auch für den Fall der Wartung.
- Firewalls:
    - Belonio arbeitet mit den Amazon Web Services Security Groups zusammen, um sicherzustellen, dass die in der Amazon Web Services-Umgebung laufenden Dienste nur für die Netzwerke zugänglich sind, die sie benötigen. Der Zugriff auf die Netzwerk-Ports der verschiedenen Dienste wird soweit eingeschränkt, dass der Zugriff nur durch die Dienste möglich ist, die den Zugriff benötigen.
- Belonio folgt AWS Software-/Infrastruktur Standards und erfüllt diese in regelmäßigen Abständen. Darunter u.a.:
    - AWS Foundational Technical Review
    - CIS AWS Foundations Benchmark standard
- Belonio verwendet verschiedene Monitoring-Tools, um die maximale Verfügbarkeit, Leistung und Sicherheit der Anwendung durch Amazon Web Services (z.B. CloudWatch) zu gewährleisten. Die Überwachung umfasst unter anderem die folgenden Parameter:
    - Verfügbarkeit
        - Verfügbarkeit der Dienste der Anwendung
        - Zugänglichkeit von Backend-Systemen und -Diensten
    - Ressourcen
        - CPU-Auslastung
        - Auslastung der Netzwerkschnittstellen
        - Nutzung von persistentem und flüchtigem Speicher
    - Leistung
        - Antwortzeiten der Anwendung
        - Antwortzeiten der Backend-Systeme
        - Abfragezeiten für Datenbankinhalte

        - Sicherheit
            - Status der Systeme aktualisieren
            - Error logs Access logs Backups
- Zusätzliche Maßnahmen mit Blick auf das Risiko vermeintlich legaler Zugriffe in den USA als Sitz des Mutterkonzerns von Amazon Web Services EMEA SARL (u.a. auf Basis von Section 702 FISA, EO 12.333 (und PPD-28) sowie des Cloud Acts):
    - relevante Zertifizierungen (u.a. BSI C5, FIPS-140, ISO-27001) für Rechenzentren und Managed Services
    - AWS Control Tower zur Sicherstellung der Einhaltung von Sicherheitsrichtlinien
    - AWS KMS, eine FIPS-2/teils 3 zertifizierte Hardware Security Key Infrastruktur erzeugt einen kryptografischen Schlüssel für die Verschlüsselung aller Daten AT-Rest. Der KMS läuft in einem separaten abgesicherten Konto.
    - CloudTrail zeichnet alle Vorgänge in den AWS Konten zentral auf. Logfiles werden in einem separaten Konto aufgezeichnet und sind vor Manipulation geschützt
    - GuardDuty überwacht die Infrastruktur ständig auf verdächtigen Datenverkehr

Anlage 2 zur Auftragsverarbeitung – Zugelassene Unterauftragsverarbeiter und Auftragsinhalte

Insofern Datenübermittlungen an Unterauftragsverarbeiter in Drittländern gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments Teil der Auftragsverarbeitung sind, erfolgen diese auf Basis der Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.
Die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit für die Übermittlung personenbezogener Daten an Drittländer sind in Anlage 1 aufgeführt.

Unterauftragsverarbeiter für die Bereitstellung der webbasierten Portallösung für Zuwendungen (Benefits) zum Barlohn:

- Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg
    - Hosting, Datenverarbeitung und Speicherung (auf den AWS-Servern in Europa / Frankfurt)
- Easybill GmbH, Düsselstraße 21, 41564 Kaarst, Deutschland
    - Rechnungslegung
- Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, D04 V4X7, Ireland
    - Mögliche kurzzeitige Speicherung (via AES256-Bit-Verschlüsselung) von individuell durch den Auftraggeber angeforderten Sonderreports in der GoogleDrive
- Userlane GmbH, Rosenheimerstraße 143C, 81671 München, Deutschland
    - Unterstützung bei der Systemführung, Bedienungshilfe
- Widas ID GmbH, Maybachstraße 2, 71299 Wimsheim, Deutschland
    - Cloud Identity & Access Management

Benefit-Partner für die Ausschüttung von Zuwendungen (Einschlägigkeit bestimmt sich nach den Bestimmungen zur Leistung im Hauptvertrag):

- Edenred Deutschland GmbH, Claudius-Keller-Str. 3c, 81669 München
    - Bereitstellung und Aufladung von Ticket Plus Karten by Belonio
    - Bereitstellung und Aufladungen von Gutscheinen im Gutscheinpool und MyBen
- 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 Sortiment 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

- Eleasa, eine Marke der el Leasing & Service AG, Ubbenstraße 15, 30159 Hannover
    - Bereitstellung von und Beratung zu Diensträdern und Hardware für Mitarbeiter. Rückmeldung der relevanten Daten zum Leasing des Fahrrad oder der Hardware zur Erstellung von Reportings.
- Purobike GmbH - Radelnde Mitarbeiter, Krögerweg 33, 48155 Münster
    - Bereitstellung von und Beratung zu Diensträdern
    - Rückmeldung der relevanten Daten zum Leasing Fahrrad zur Erstellung von Reportings

Anlage 3 zur Auftragsverarbeitung – Beschreibung des Gegenstands der Verarbeitung, Zwecks und Umfangs sowie der Kategorien der Daten der Auftragsverarbeitung

Die folgenden Ausführungen beschreiben den für den Regelfall festgelegten Gegenstand der Verarbeitung, Kategorien der Daten sowie den Zweck und Umfang der Auftragsverarbeitung aus § 2.

Gegenstand der Verarbeitung:

Belonio hat eine webbasierte Portallösung bestehend aus dem Belonio-Cockpit (Verwaltungsschnittstelle für den Auftraggeber) und einer Anwendung / App (zur Nutzung durch die Mitarbeiter des Auftraggebers) entwickelt, die dem Auftraggeber den Einsatz von Zuwendungen zum Barlohn seiner Mitarbeiter ermöglicht. Die Mitarbeiter des Auftraggebers verwenden als Nutzer die Anwendung / App um auf Zuwendungen zuzugreifen.

Art und Zweck der Verarbeitung:

1) Die Stammdaten des einzelnen Mitarbeiters werden zwecks der Registrierung und Hinterlegung im System durch den Auftraggeber in der auf den AWS-Servern gehosteten Portallösung eingetragen oder per Datei-Import eingespielt. Darüber hinaus wird zur Nutzung die E-Mail-Adresse der Mitarbeiter für den Zugang zur App benötigt.

2) Bei der Nutzung der App durch die Mitarbeiter werden zusätzlich relevante Daten für die rechtskonforme Gewährung der steuerfreien Sachbezüge sowie die Rechnungslegung und Erstellung von Nachweisen auf Anfrage des Auftraggebers verarbeitet.

Art der personenbezogenen Daten:

Zu 1): Personalnummer, Anrede, Vorname, Nachname, Geburtsdatum, E-Mail-Adresse, Name des Arbeitgebers.

Zu 2): Zuflusszeitpunkt der einzelnen Zuwendungen (Benefits), z.T. fotografische Belegerfassung, Historie über Zuwendungszufluss.

Für Ansprechpartner und im Belonio-Cockpit als Administrator bestimmte natürliche Personen (Benefit-Piloten): Name, Vorname, geschäftliche Telefonnummer, E-Mail-Adresse und ggf. weitere Kontaktinformationen des Ansprechpartners / der Ansprechpartnerin beim Auftraggeber.