Leistungsbeschreibung

Leistungsbeschreibung

Die BLS Bikeleasing-Service Österreich GmbH („Anbieter“) bietet eine Software-Lösung an, die es dem Kunden deutlich erleichtert, den Essenszuschuss an Mitarbeiter zu übergeben. Die Software-Lösung umfasst zwei Module: Das Arbeitgeber-Portal und die Mitarbeiter-App.
Admin-Nutzer des Kunden erhalten Zugriff auf das Arbeitgeber-Portal zur einfachen Freischaltung, Verwaltung und Abrechnung des Essenszuschuss.
Im Arbeitgeber-Portal konfigurierte Freischaltungen werden mit Hilfe der Mitarbeiter-App digital an den entsprechenden Mitarbeiter übermittelt. Mitarbeiter erhalten Zugriff auf die Mitarbeiter-App zur Nutzung des Essenszuschuss, einschließlich der Möglichkeit zur digitalen Belegeinreichung. Die Mitarbeiter-App ist dabei auch als Web-Anwendung verfügbar.

Der Anbieter wird durch den Kunden mittels dieses Leistungsvertrags zu folgenden Leistungen beauftragt:

Arbeitgeber-Portal
Der Anbieter stellt dem Kunden eine webbasierte Verwaltungssoftware zur Verfügung.
Hier stehen den Admin-Nutzern des Kunden insbesondere folgende Funktionalitäten zur Verfügung:

- Login via E-Mail und Passwort
- SSO-Login via Microsoft mit 2FA
- SSO-Login via Google und Apple
- Ändern und Einsehen der Konfiguration und Freischaltung des Essenszuschuss für einzelne Mitarbeiter des Kunden
- Den Essenszuschuss für Mitarbeiter stoppen bzw. ein Enddatum setzen
- Die Anzahl der bezuschussten Mahlzeiten pro Monat festzulegen (maximal 15)
- Die maximale Erstattungshöhe pro Mahlzeit festzulegen.
- Mitarbeiter als ausgeschieden markieren
- Mitarbeiterdaten löschen
- Herunterladen der Abrechnungsdatei für die monatliche Gehaltsabrechnung
- Herunterladen des Reports zur Dokumentation im Lohnkonto
- Einstellungen zum automatischen Versand der Abrechnungsdatei per E-Mail an bis zu drei E-Mail-Adressen
- Digitale Einsicht in durch Mitarbeiter eingereichte Belege sowie eigenständige Bestätigung oder Ablehnung von diesen

Der Kunde kann über das Arbeitgeber-Portal der Plattform alle Mitarbeiter oder Mitarbeitergruppen zur Gewährung des Essenszuschusses über die Mitarbeiter-App freischalten.

Der Anbieter bietet dem Kunden drei Möglichkeiten, neue Nutzer zu registrieren:

Option 1: Generierung von individuellen Registrierungscodes
Der Anbieter erstellt für den Kunden eine individuell generierte Liste von Registrierungscodes. Die Registrierungscodes enthalten folgende Daten: ID des Kunden und Personalnummer des Mitarbeiters. Die Registrierungscodes können nur durch den Anbieter entschlüsselt werden. Der Anbieter übermittelt dem Kunden eine Liste, die die Zuordnung von Registrierungscodes zu Personalnummer des Mitarbeiters ermöglicht (wird zum Versand des Serienbriefs vom Arbeitgeber benötigt).

Option 2: Generierung eines allgemeinen Registrierungscodes
Der Anbieter erstellt für den Kunden einen unternehmensübergreifenden Registrierungscode, über welchen der Nutzer sich registrieren kann. Der Anbieter kann die Nutzer auf Basis der eingegebenen Daten (Anrede, Vorname und Nachname) überprüfen und freischalten.

Option 3: Freischalten per E-Mail
Der Anbieter bietet die Möglichkeit, neue Nutzer per E-Mail einzuladen. Der Kunde kann hierzu die E-Mail-Adressen manuell im Arbeitgeber-Portal hinzufügen oder diese dem Anbieter für einen Excel-Import zur Verfügung stellen.

Digitales Hochladen von Belegen und Belegprüfung
Ein als Nutzer registrierter Mitarbeiter des Kunden erhält einen individuellen Zugang zu der Mitarbeiter-App. Wenn für ihn über das Arbeitgeber-Portal der Essenszuschuss freigeschaltet ist, kann er direkt über die App Mahlzeiten-Belege

einreichen. Für die Einreichung muss ein Foto der Rechnung oder des Belegs hochgeladen und im Anschluss folgende Informationen eingegeben werden:

- Datum der Mahlzeit
- Betrag der Mahlzeit
- Welche Positionen des Belegs waren Teil der Mahlzeit. Diese Angabe ist nur im Fall eines Mischbelegs notwendig.
- Angabe, ob der Beleg einer Gaststätte beziehungsweise dem zugehörigen Lieferdienst entstammt

Jeder so hochgeladene Beleg wird in der App geprüft. Die Prüfung geschieht nach Wahl des Anbieters manuell durch Mitarbeiter des Anbieters oder vollautomatisiert durch eine hierfür geeignete KI. Im Fall einer vollautomatisierten Prüfung durch KI wird jedoch stichprobenartig und in Zweifelsfällen eine ergänzende manuelle Prüfung durch Mitarbeiter des Anbieters durchgeführt. Folgende Kriterien werden geprüft:

- Angegebenes Datum ist das Belegdatum
- Beleg stammt aus Österreich. Dies wird entweder über die Umsatzsteuer ID des Belegausstellers, oder eine Adresse auf dem Beleg überprüft.
- Der Beleg oder die vom Mitarbeiter definierten Positionen des Belegs enthalten keine alkoholischen Getränke.
- Der Beleg oder die vom Mitarbeiter definierten Positionen des Belegs enthalten keine Non Food Produkte (z.B.: Pfand, Einkaufstüten, Spielzeuge etc.).
- Belegursprung ist eine Gaststätte beziehungsweise zugehöriger Lieferdienst im Falle eines Essenszuschusses höher als 2,00€ bis maximal 8,00€

Falls Belege nicht den Prüfkriterien entsprechen, werden diese abgelehnt. Abgelehnte Belege können erneut zur Prüfung hochgeladen werden, wobei alle zuvor festgelegten Kriterien, wie beispielsweise das Datum, nach Bedarf überarbeitet werden können.

Aus den (positiv geprüften) Einzelbuchungen erstellt der Anbieter monatlich eine kumulierte Abrechnungsdatei über die Summe der zu versteuernden bzw. steuerfreien Zuschüsse je Mitarbeiter mit Bezeichnung der Lohnarten. Im Folgemonat erfolgt die Übernahme in die Lohn-/(Gehalts-)abrechnung und damit die Erstattung an den Mitarbeiter. Der Anbieter prüft hierfür alle Belege des laufenden Monats bis zum 6. Kalendertag des Folgemonats, so dass diese in der Export-Datei bei erfolgreicher Prüfung berücksichtigt sind.

Abgelehnte Belege werden nicht auf den für den jeweiligen Mitarbeiter festgelegten Höchstbetrag angerechnet und sind im Export für die Lohnabrechnung nicht enthalten. Etwas anderes gilt nur, wenn der Arbeitgeber diese Belege trotz Ablehnung durch den Anbieter seinerseits manuell im Portal freigegeben hat.

Die von den Mitarbeitern hochgeladenen Belege werden vom Betreiber der App in digitaler Form für bis zu 10 Jahre aufbewahrt, um eine langfristige Dokumentation zu gewährleisten. Diese Daten können im Falle einer Prüfung auf Anforderung des Arbeitgebers als Export-Datei zur Verfügung gestellt werden, zusätzlich zu den bereits im Arbeitgeberportal bereitgestellten Reports. Der Auftrag zur 10-jährigen Speicherung kann auf Wunsch des Kunden jederzeit widerrufen werden; in diesem Fall werden anschließend alle Daten aus allen Systemen des Anbieters gelöscht.

Weitere Details zur Software

Mitarbeiter: Mitarbeiter-App
Der Mitarbeiter identifiziert sich über einen eigenen Zugang zur Mitarbeiter-App (auch zugänglich als Web-Anwendung), mit dem er ausschließlich die ihn betreffenden Vorgänge einsehen kann, die sein Arbeitgeber ihm zur Verfügung stellen will.
In der Mitarbeiter-App wird insbesondere der entsprechende Essenszuschuss dem Mitarbeiter digital angezeigt. Für den Nachweis über die ordnungsgemäße Verwendung des Zuschusses ist der Mitarbeiter verantwortlich. Zu diesem Zweck muss der Mitarbeiter für jede Mahlzeit Belege hochladen und bestätigen, dass die von ihm hierzu systemseitig geforderten Angaben zutreffend sind.

Folgende Vorgänge kann der Mitarbeiter in der Mitarbeiter-App einsehen oder beeinflussen:

Leistungsbeschreibung

- Der Mitarbeiter sieht in seiner Mitarbeiter-App im Nachhinein, in welcher Höhe ihm vom Arbeitgeber anhand seiner tatsächlichen Arbeitstage ein Essenszuschuss im vorangegangenen Monat gewährt wird.
- Der Mitarbeiter kann ein Foto des Belegs hochladen oder direkt in der Mitarbeiter-App fotografieren.
- Nach Hochladen des Belegs kann der Mitarbeiter den Betrag der Mahlzeit und das Datum der Rechnung eingeben.
- Nach Eingabe der erforderlichen Daten wird dem Mitarbeiter in der Mitarbeiter-App eine Zusammenfassung inklusive Betrag der Mahlzeit und Datum der Rechnung angezeigt. Durch die Wahl aus den zwei Feldern „Einzelbeleg“ und „Mischbeleg“ kann der Mitarbeiter hierbei zudem die Art des hochgeladenen Belegs angeben. Zusätzlich kann hier in einem Kommentarfeld ein Kommentar eingegeben werden. Bei einem Mischbeleg ist im Kommentarfeld zwingend einzutragen, welche Komponenten des Belegs Bestand der zu erstattenden Mahlzeit waren.
- Die Einzelbelegprüfung erfolgt durch Angestellte des Anbieters oder vollautomatisiert durch KI mit manuellen Stichproben.
- Der Mitarbeiter sieht in seiner Mitarbeiter-App inklusive Angabe des Datums, welcher Beleg freigegeben und ausgezahlt wird.
- Der letztendliche Essenszuschuss-Betrag, der zusätzlich zum Gehalt ausgezahlt wird, kann vom Mitarbeiter jederzeit in der App eingesehen werden.

Weitere Funktionalitäten der Mitarbeiter-App
In der Mitarbeiter-App stehen weiter folgende Funktionen zur Verfügung:

- Persönliche Daten einsehen und ändern: Anrede, Titel, Vorname und Nachname
- Sprache ändern
- Passwort ändern
- Passwort zurücksetzen: Hierfür wird im Rahmen der Registrierung die E-Mail-Adresse des Nutzers abgefragt
- Darstellungsfarbe
- Benachrichtigungseinstellungen
- Zugriff auf etwaige weitere vom Arbeitgeber freigeschaltete Benefits

Arbeitgeber: Arbeitgeber-Portal zur Verwaltung
Der Arbeitgeber verwaltet den Essenszuschuss und andere Benefits über das vom Anbieter zur Verfügung gestellte Arbeitgeber-Portal.

Steuerrechtlicher Hintergrund

Die Zuwendung des Essenszuschusses über den Anbieter folgt § 3 Abs.1 Z 17 EStG, §49 Abs. 3 Z 12 ASVG, § 41 Abs. 4 lit. c FLAG und § 5 Abs. 2 lit. c KommSt.

Allgemeine Geschäftsbedingungen (AGB) für Arbeitgeber (Unternehmen)

Präambel
Die BLS Bikeleasing-Service Österreich GmbH („Anbieter“) bietet eine Software-Lösung an, die Unternehmen den Einsatz von attraktiven Mitarbeiter-Benefits („Benefits“) deutlich vereinfacht und digitalisiert. Die Software-Lösung umfasst
insbesondere das Arbeitgeberportal zur einfachen Verwaltung und Konfiguration der Benefits sowie eine zugehörige Mitarbeiter-App („App“) zur Information der Mitarbeiter über die im Arbeitgeberportal freigeschalteten Benefits, zur digitalen Nutzung ausgewählter Benefits sowie, je nach Benefit Modul, auch zur digitalen Belegeinreichung (insgesamt „Software“) und ggf. weitere Zusatzleistungen gemäß der Leistungsbeschreibung des jeweiligen Benefit Moduls. Diese Allgemeinen Geschäftsbedingungen („AGB“) regeln zusammen mit dem Vertragsdokument und dessen sonstigen Anlagen das Vertragsverhältnis („Vertrag“) zwischen dem Anbieter und dem Kunden über die kostenpflichtige Nutzung der Software. Das Verhältnis

1. Gegenstand und Zustandekommen des Vertrages

1.1. Diese AGB gelten für die Inanspruchnahme und Nutzung der Software vom Anbieter durch den Kunden sowie für etwaige weitere im Rahmen der Inanspruchnahme der jeweiligen Benefit Module vereinbarten Leistungen. Allgemeine Geschäfts- oder Einkaufsbedingungen des Kunden werden nur dann Vertragsbestandteil, wenn dies ausdrücklich in Textform vereinbart wurde.

1.2. Die Nutzung der Software wird nur Unternehmen im Sinne des § 1 UGB und keinen Verbrauchern angeboten.

2. Leistungen des Anbieters

2.1. Der Anbieter stellt die Software ausschließlich zum Abruf über das Internet durch den Kunden bereit („Software-as-a-Service“); der Kunde erhält an der jeweils aktuellen Version ein einfaches, nichtausschließliches, nicht übertragbares, nicht unterlizenzierbares und auf die Vertragslaufzeit
beschränktes Recht zur Nutzung. Betrieb und Wartung der Software obliegen dem Anbieter. Der Kunde ist berechtigt, die Software für seine eigenen Zwecke sowie für die Zwecke der mit ihm gemäß §189a Z 8 UGB verbundenen Unternehmen zu nutzen. Der Kunde ist berechtigt, seinen Mitarbeitern, gesetzlichen Vertretern, sowie Mitarbeitern und gesetzlichen Vertretern der mit ihm verbundenen Unternehmen
Zugriff zur Software zu ermöglichen („Nutzer“).

2.2. Die App ist dabei sowohl als Anwendungssoftware für Mobilgeräte (iOS und Android) als auch als Web-Anwendung verfügbar. Die Funktionen der App stützen sich auch auf Leistungen von Dritten („Drittleistungen“). Drittleistungen bestehen größtenteils aus Smartphones und Telekommunikationsleistungen (mobile Datenübertragung und Telefonservice) sowie Schnittstellen zur Analyse und Prüfung von Belegen.

2.3. Ort der Leistungsübergabe ist jeweils der Router-Ausgang des vom Anbieter für die Leistungserbringung genutzten Rechenzentrums. Der Kunde hat selbstständig dafür zu sorgen, die Leistung entgegennehmen zu können. Für die Telekommunikationsverbindung zwischen dem Kunden und dem Anbieter bis zum Router - Ausgang (Übergabepunkt) und für die Beschaffenheit der erforderlichen Hard- und Software auf Seiten des Kunden ist der Anbieter nicht verantwortlich.

2.4. Die zur Nutzung der Software erforderliche Hardware (insbesondere Smartphones) wird vom Anbieter nicht zur Verfügung gestellt.

2.5. Der Kunde hat keinen Anspruch auf Zugang zu den bzw. Übergabe der Quellcodes der Software sowie deren Dokumentation.

2.6. Details zur Leistungserbringung durch den Anbieter und etwaigen weiteren Zusatzleistungen sind in der für das jeweilige Benefit Modul geltenden Leistungsbeschreibung geregelt.

2.7. Sofern keine Mindestabnahmemenge oder eine feste Anzahl an Mitarbeiterlizenzen vereinbart wurde, ist der Kunde jederzeit berechtigt, die Anzahl der freigeschalteten Mitarbeiter sowie die Benefit Module, für die Mitarbeiter freigeschaltet wurden, zu erhöhen oder zu verringern.

2.8. Der Anbieter ist berechtigt, zur Leistungserbringung Subunternehmer als Erfüllungsgehilfen zu beauftragen. Eventuelle weitergehende datenschutzrechtliche Verpflichtungen gegenüber dem Kunden bleiben unberührt.

2.9. Der Anbieter stellt den für die ordnungsgemäße Nutzung der Benefit Module erforderlichen Speicherplatz zur Verfügung.

3. Mindestlizenzmodelll

3.1. Sofern im Angebot oder im Bestellformular ausdrücklich eine Mindestanzahl an Lizenzen vereinbart wird, verpflichtet sich der Kunde zur Abnahme
und Zahlung einer Mindestanzahl an Mitarbeiterlizenzen pro
Monat, für eine Festlaufzeit von drei Monaten, unabhängig von der tatsächlichen Nutzung oder Freischaltung einzelner Benefits durch Mitarbeitende
.

3.2. Der Vertrag hat ab Vertragsbeginn (Startdatum) eine Laufzeit von drei Monaten (Festlauzeit). Der Vertrag verlängert sich jeweils um einen weiteren Monat, wenn er nicht von einer Partei mit einer Frist von 14 Tagen zum Monatsende, erstmals möglich zum Ablauf zum Monatsende der Festlaufzeit, in Textform gekündigt wird. Eine Kündigung aus wichtigem Grund bleibt unberührt.
Nach Ablauf der Festlaufzeit kann der Kunde die Anzahl der Lizenzen jederzeit mit Wirkung ab Beginn des Folgemonats, ohne den gesamten Vertrag zu beenden, anpassen. Eine Erhöhung der Lizenzanzahl ist durch den Kunden jederzeit über das Arbeitgeberportal digital möglich. Diese erhöht nicht die vereinbarte Mindestlizenzanzahl nach Absatz 1, es sei denn, dies wird ausdrücklich und in Textform vereinbart. Eine Reduzierung der Mindestlizenzanzahl ist in Textform per E-Mail an den zuständigen
Vertriebsmitarbeiter oder an support@probonio.at möglich. Die Reduktion wird mit Wirkung zum jeweils nächsten Abrechnungsmonat wirksam, sofern sie bis zum 15. Kalendertag des Vormonats eingeht.

3.3 Im Fall einer Reduzierung der Mindestlizenzanzahl behält sich der Anbieter vor, etwaige gewährte Rabatte für die verbleibenden Lizenzen entsprechend anzupassen oder komplett zu streichen. Die Änderung der Rabattsätze wird dem Kunden vorab transparent kommuniziert.

3.4. Soweit keine ausdrückliche Vereinbarung über eine Mindestlizenzanzahl vorliegt, gelten die Regelungen gemäß Ziffer 2.7.

4. Systemvoraussetzungen

4.1. Soweit nicht ausdrücklich abweichend vereinbart, unterstützt der Anbieter für die Web-Oberfläche der Software ausschließlich die jeweils letzte und vorletzte vom Hersteller unterstützte sowie als stabil und für den Produktionseinsatz freigegebene, marktübliche Browsersoftware und Desktop-Betriebssysteme maximal bis zum Ablauf des allgemeinen Herstellersupports.

4.2. Die App wird über den jeweiligen App-Store zur Verfügung gestellt. Für die Nutzung der App ist jeweils ein voll funktionsfähiges Smartphone eines gängigen Herstellers mit einem aktuellen Betriebssystem (iOS oder Android, letzte und vorletzte vom Hersteller unterstützte Version) erforderlich. Der Kunde bzw. der Nutzer muss die App selbständig auf den entsprechenden Smartphones installieren und die Berechtigungen für Foto-Funktionen und Push-Benachrichtigungen freigeben. Um die vollständige Funktionsweise sicherzustellen, muss die jeweils aktuelle Version installiert und benutzt werden.

5. Verfügbarkeit/Support

5.1. Die Software hat auf Jahresbasis eine technische Verfügbarkeit von mindestens 99%, wobei angemessene und vorab mitgeteilte Zeiten geplanter Nichtverfügbarkeit (etwa wegen Wartungsarbeiten) nicht berücksichtigt werden. Zusätzlich ist eine geplante Nichtverfügbarkeit
zweiwöchentlich am Mittwoch zwischen 18.00 und 22.00 Uhr vereinbart.

5.2. Der Anbieter bietet zu den Geschäftszeiten (Montag - Freitag von 9.30 – 16.30 Uhr mit Ausnahme der gesetzlichen Feiertage sowie dem 24. und 31. Dezember) Kundensupport und Entstörungsleistungen an. Der Support ist über die Software (Feedback-senden Funktion), per E-Mail unter support@probonio.at und in dringenden Fällen telefonisch unter +43 512/ 219 321 -70 erreichbar.

5.3 Ein Support ist ausgeschlossen,

- bei Fehlern, die durch unautorisierte Modifikation der Software verursacht wurden;
- bei Fehlern, die auf Grund höherer Gewalt, fehlerhafter Stromversorgung oder sonstigen Umweltbedingungen verursacht wurden;

- bei jeglichen Hardwaredefekten;
- für die Entfernung von Schadsoftware.

6. Rechte des Anbieters, Zusammenarbeit mit Partnern, Referenzkunden

6.1. Der Kunde ist für die Einhaltung der steuerlichen Vorschriften und die sich hieraus ergebenden Verpflichtungen durch die Gewährung der Benefits selbst verantwortlich.
Der Anbieter ist aber berechtigt, Angebote und Dienste in ihrer Verfügbarkeit einzuschränken oder ganz aufzugeben, wenn Angebote und Dienste des Anbieters nicht mehr den aktuellen steuerlichen oder sonstigen Gesetzesvorgaben entsprechen oder begründete Zweifel hieran bestehen.

6.2. Der Anbieter ist berechtigt, den Zugang des Kunden oder Nutzers zu der Software zu sperren, wenn
6.2.1. begründete Anhaltspunkte bestehen, dass die Zugangsdaten des Kunden missbraucht wurden oder werden oder die Zugangsdaten einem unbefugten Dritten überlassen wurden oder werden oder Zugangsdaten durch mehr als eine natürliche Person verwendet werden;
6.2.2. begründete Anhaltspunkte bestehen, dass sich Dritte anderweitig Zugang zu der dem Kunden bereitgestellten Software verschafft haben;
6.2.3. begründete Anhaltspunkte bestehen, dass eine konkrete Nutzung der Software durch den Kunden oder Nutzer die Sicherheit der Software und/oder andere Kundendaten bedroht;
6.2.4. der Anbieter gesetzlich, gerichtlich oder behördlich zur Sperrung verpflichtet ist oder
6.2.5. der Kunde mehr als vier Wochen mit der Zahlung des vereinbarten Entgelts in Verzug ist. Der Anbieter soll dem Kunden eine Sperrung spätestens drei Werktage vor Inkrafttreten der Sperrung in Textform ankündigen, soweit die Ankündigung unter Abwägung der beiderseitigen Interessen zumutbar und mit dem Zweck der Sperrung vereinbar ist.

6.3. Soweit der Anbieter dem Kunden einen kostenlosen Zugriff auf Application Programming Interfaces („API“) gewährt, handelt es sich um eine freiwillige und jederzeit widerrufliche Zusatzleistung, sofern die Parteien nichts anderes vereinbart haben. Insbesondere ist der Anbieter ohne eine anderweitige vertragliche Regelung berechtigt, die API in neuen Versionen anzubieten und ältere Versionen der API einzustellen.

6.4. Sofern nicht anders geregelt, verbleiben alle Rechte an Daten, die in die Systeme des Anbieters hochgeladen oder innerhalb dieser Systeme generiert werden ("Kundendaten"), beim Kunden.

6.5. Der Anbieter arbeitet im Rahmen von einzelnen Benefit Modulen mit Partnern zusammen, indem es die Produkte oder Dienstleistungen dieser Partner erwirbt und an die Kunden weiterveräußert oder die Vertragsanbahnung zwischen dem Kunden und dem Partner unterstützt. Bei solchen von Partnern zur Verfügung gestellten Produkten oder Dienstleistungen gelten die AGB des jeweiligen Partners ergänzend, sofern diese einbezogen wurden.

6.6. Der Kunde räumt dem Anbieter das nicht ausschließliche, nicht übertragbare, auf die Dauer der Zusammenarbeit beschränkte Recht ein, im Rahmen der gewerblichen Tätigkeit, ungeachtet der Übertragungs-, Träger -und Speichertechniken, den Kunden als Kunden des Anbieters unter Verwendung des Firmennamens und evtl. Firmenlogos als Referenzkunden zu nennen. Hierzu stellt der Kunde dem Anbieter auf Anforderung in Textform das Firmenlogo des Kunden digital zur Verfügung (als JPG, PNG oder Vektorgrafik). Der Kunde versichert, Inhaber der Rechte (Urheber- und/oder Markenrechte) zu sein. Der Anbieter ist berechtigt, den Firmennamen und evtl. Firmenlogos des Kunden zu Referenz- und Werbezwecken zu verwenden, z. B. durch Nennung auf der Website des Anbieters, in Präsentationen oder in Marketingmaterialien. Die Einwilligung des Kunden erfolgt freiwillig und kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Der Widerruf hat in Textform zu erfolgen. Sollte ein Rückgängigmachen allenfalls bereits vorgenommener Veröffentlichungen aus technischen und/oder praktischen Gründen (z.B. bereits erfolgte Veröffentlichung in Printmedien etc.) nach dem Zugang der Widerrufserklärung nicht möglich sein, können daraus keine Ansprüche des Kunden abgeleitet werden. Der Kunde erhält das nicht ausschließliche, nicht übertragbare, auf die Dauer der Zusammenarbeit beschränkte Recht, den Firmennamen und evtl. Firmenlogos des Anbieters sowie Screenshots aus der Benefit-App zu Werbezwecken zu nutzen, z. B. im Rahmen des Employer Brandings auf der eigenen Karriereseite des Kunden oder in Social-Media-Kanälen des Kunden. Eine weitergehende inhaltliche Darstellung der Zusammenarbeit, z. B. unter Nennung konkreter Maßnahmen, Kennzahlen oder individueller Vereinbarungen, bedarf der vorherigen Zustimmung der jeweils anderen Partei in Textform.

7. Pflichten des Kunden

7.1. Es obliegt dem Kunden, sicherzustellen, die für den Betrieb der Software erforderlichen Systemvoraussetzungen zu erfüllen.

7.2. Der Kunde verpflichtet sich dazu, die Funktionsanleitung der App zu befolgen und die Nutzer entsprechend anzuweisen.

7.3. Der Kunde hat die Zugangsdaten zu der Software sicher zu verwahren und darf diese nur jeweils berechtigten Mitarbeitern zugänglich machen. Der Kunde verpflichtet sich, seine Mitarbeiter zum vertraulichen Umgang mit den Zugangsdaten zu verpflichten und den Anbieter unverzüglich in Kenntnis setzen, wenn der Verdacht besteht, dass die Zugangsdaten unbefugten Personen bekannt geworden sein könnten.

7.4. Wenn der Kunde über APIs (siehe Ziffer 6.3) oder in sonstiger Weise Daten in die Systeme von des Anbieters übermittelt, ist der Kunde dafür verantwortlich, dass diese Daten keine Bestandteile enthalten, die in den Systemen des Anbieters Funktionsstörungen oder Schäden verursachen oder verursachen können (z.B. Viren, Trojaner oder sonstiger schadhafter Code) und hat hierzu dem Stand der Technik entsprechende Schutzprogramme einzusetzen.

7.5. Der Kunde verpflichtet sich, bei der Verwendung der Software sämtliche anwendbaren rechtlichen Vorschriften, insbesondere des Urheber- und Datenschutzrechts, zu beachten.

7.6. Der Kunde für die Einhaltung der steuerlichen Vorschriften und die sich hieraus ergebenden Verpflichtungen durch die Gewährung der Benefits selbst verantwortlich.

8. Entgelte

8.1. Der Kunde zahlt an den Anbieter für die Nutzung der Software das im Vertrag vereinbarte Entgelt.

8.2. Soweit nicht abweichend vereinbart, gelten die Entgelte monatlich und netto zzgl. anwendbarer Umsatzsteuer. Die monatliche Vergütung für die jeweiligen Benefits fällt für jeden Monat an, in dem diese freigeschaltet sind. Skonto wird nicht gewährt.

8.3. Die in Rechnung gestellten Entgelte sind mit ordnungsgemäßer Rechnungsstellung nach 14 Tagen fällig.

8.4. Bei einer vertraglich vereinbarten Mindestlizenzanzahl (Mindestlizenzmodell) erfolgt die monatliche Abrechnung mindestens auf Basis der vereinbarten Mindestanzahl, unabhängig von der tatsächlichen Freischaltung oder Nutzung durch Mitarbeitende des Kunden.

9. Rechte des Kunden bei Mängeln, Anzeigepflichten

9.1. Der Anbieter gewährleistet die Funktions- und Betriebsbereitschaft der Software nach den Bestimmungen des Vertrages.

9.2. Der Kunde hat dem Anbieter auftretende Mängel nach deren Bekanntwerden unverzüglich in Textform, etwa per E-Mail oder über die Feedback-senden-Funktion, anzuzeigen. Weiterhin wird der Kunde den Anbieter bei der Behebung von Mängeln in angemessener Weise unentgeltlich unterstützen und den Anbieter, soweit zumutbar, insbesondere sämtliche Informationen und Dokumente zukommen lassen, die der Anbieter für die Analyse und Beseitigung von Mängeln benötigt.

9.3. Sind die vom Anbieter nach diesem Vertrag zu erbringenden Leistungen mangelhaft, wird der Anbieter innerhalb angemessener Frist nach Zugang einer Mängelrüge des Kunden die Leistungen nach seiner Wahl nachbessern oder die Software ersetzen. Als Nachbesserung gilt auch die Bereitstellung von Nutzungsanweisungen, mit denen der Kunde (sowie ggf. die Nutzer) aufgetretene Mängel vorübergehend zumutbar umgehen kann, um die Software vertragsgemäß zu nutzen. In dem Fall hat der Anbieter die eigentliche Fehlerursache in angemessener Zeit durch Anpassungen der Software zu beseitigen.

9.4. Schlägt die mangelfreie Erbringung der Leistungen aus Gründen, die der Anbieter zu vertreten hat, auch innerhalb einer vom Kunden in Textform gesetzten angemessenen Frist fehl, kann der Kunde die vereinbarte Vergütung um einen angemessenen Betrag mindern. Den Höchstbetrag stellt die für den jeweiligen Zeitraum vereinbarte Lizenzgebühr des mangelhaft erbrachten Benefit Moduls für den jeweiligen Nutzer dar.

9.5. Erreicht die Minderung nach Ziffer 9.4 in zwei aufeinander folgenden Monaten oder in zwei Monaten eines Quartals den in Ziffer 9.4 genannten Höchstbetrag, kann der Kunde den Vertrag ohne Einhaltung einer Frist kündigen. Das Recht zur Kündigung aus wichtigem Grund wird durch diese Bestimmung nicht eingeschränkt.

9.6. Im Falle von Rechtsmängeln steht es dem Anbieter frei, die betroffenen Bestandteile der Software entweder nachträglich zu lizenzieren oder diese gegen äquivalente Bestandteile auszutauschen, soweit hierdurch der Funktionsumfang der Software nicht oder nur unwesentlich beeinträchtigt wird.

9.7. Die Aufrechnung gegenüber Forderungen des Anbieters ist für den Kunden beschränkt auf Gegenforderungen, die unbestritten oder rechtskräftig zuerkannt sind oder die in einem synallagmatischen Verhältnis zu dem jeweils betroffenen Anspruch stehen.

10. Haftung und Haftungsbeschränkung

10.1. Der Anbieter haftet unbeschränkt für vorsätzlich oder fahrlässig durch den Anbieter, seine gesetzlichen Vertreter oder Erfüllungsgehilfen verursachte Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.

10.2. Der Anbieter haftet weiter für Schäden, die der Anbieter, seine gesetzlichen Vertreter oder Erfüllungsgehilfen durch vorsätzliches oder grob fahrlässiges Verhalten verursacht haben. In Fällen leichter Fahrlässigkeit haftet der Anbieter nur bei Verletzung einer wesentlichen Vertragspflicht durch den Anbieter, gesetzliche Vertreter des Anbieters oder durch Erfüllungsgehilfen des Anbieters. Eine wesentliche Vertragspflicht im Sinne dieser Ziffer ist eine Pflicht, die entscheidend für den Abschluss des Vertrages war oder deren Erfüllung die Durchführung des Vertrages erst ermöglicht und auf deren Erfüllung sich der Vertragspartner deswegen regelmäßig verlassen darf. Hierzu zählt insbesondere die Bereitstellung der Software und deren Funktionsfähigkeit.

10.3 Die Haftung gemäß der vorstehenden Ziffer 10.2 ist bei leichter Fahrlässigkeit auf den im Zeitpunkt des Vertragsschlusses typischen, vorhersehbaren Schaden begrenzt. Bei vorsätzlichem Fehlverhalten eines Nutzers ist bei leichter Fahrlässigkeit eine Haftung des Anbieters aus daraus resultierenden Schäden ausgeschlossen.

10.4. Eine etwaige Haftung des Anbieters für gegebene Garantien, für Ansprüche auf Grund des Produkthaftungsgesetzes sowie nach Ziffer 10 oder 101 bleibt unberührt.

10.5. Eine weitergehende Haftung des Anbieters ist ausgeschlossen.

11. Laufzeit und Kündigung

11.1 Soweit nicht abweichend vereinbart, hat der Vertrag eine Mindestvertragslaufzeit von einem Monat.

11.2. Soweit nicht abweichend vereinbart, verlängert sich der Vertrag um jeweils einen Monat, wenn der Vertrag nicht mit einer Frist von 14 Tagen zum Ende der jeweiligen Laufzeit durch eine der Parteien gekündigt wird.

11.3. Der Anbieter ist weiterhin berechtigt, den Vertrag fristlos zu kündigen, wenn der Kunde länger als sechs Wochen mit der Zahlung des vereinbarten Entgelts in Verzug ist und der Anbieter die Kündigung mit einer Frist von zwei Wochen zum Inkrafttreten der Kündigung in Textform dem Kunden gegenüber angedroht
hat.

11.4. Die Kündigung aus wichtigem Grund bleibt für beide Parteien unberührt.

11.5. Kündigungen bedürfen der Textform.

12. Änderung der AGB

12.1 Der Anbieter ist berechtigt, Regelungen dieser AGB einseitig zu ändern, solange diese Änderung dem Kunden zumutbar ist. Das ist insbesondere der Fall, wenn es sich um unwesentliche Änderungen handelt und ein berechtigtes Interesse des Anbieters an einer Änderung vorliegt. Einseitige Änderungen dürfen nicht die Hauptleistungspflichten der Parteien betreffen.

12.2. Unbeschadet der Regelung in Ziffer 12.1 werden Änderungen dieser AGB Vertragsbestandteil, wenn der Kunde nach Hinweis auf die Änderung und der Möglichkeit der Kenntnisnahme der Änderung innerhalb einer Frist von vier Wochen nicht in Textform widerspricht. Eine Möglichkeit der Kenntnisnahme der Änderung besteht dabei nur, wenn es dem Kunden möglich ist, die vorgesehenen neuen AGB einschließlich der Änderungen in lesbarer Form zu speichern oder auszudrucken. Der Anbieter ist verpflichtet, den Kunden vier Wochen vor dem geplanten Inkrafttreten

über die Änderungen und die Möglichkeit sowie Form, Frist und Folgen des Widerspruchs zu informieren und insbesondere auf die Bedeutung seines Schweigens und den Zeitpunkt des beabsichtigten Wirksamwerdens der Änderungen hinzuweisen. Widerspricht der Kunde, gelten die bisherigen Bedingungen fort.

13. Schlussbestimmungen
13.1. Änderungen und Nebenabreden zu diesem Vertrag bedürfen der Textform, soweit in Ziffer 14 nichts anderes geregelt ist.

13.2. Es gilt österreichisches Recht unter Ausschluss des UN-Kaufrechts und kollisionsrechtlicher Regelungen.

13.3. Erfüllungsort ist Innsbruck. Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist Innsbruck, sofern ein anderer Gerichtsstand nicht zwingend gesetzlich vorgegeben ist.

13.4. Bei Widersprüchen zwischen diesen AGB und individuellen Vertragsbestandteilen (z.B. Angebot, Bestellformular) gehen die individuell vereinbarten Regelungen vor.

Technisch-organisatorische Maßnahmen

des Unternehmens: BLS Bikeleasing-Service Österreich GmbH

Adresse: Exlgasse 24, Innsbruck 6020

Für die folgenden Angaben wird die Richtigkeit bestätigt.

Innsbruck, 21.10.2025

Ort & Datum

Unterschrift

0. Präambel

BLS Bikeleasing-Service Österreich GmbH ist eine 100% Tochter des deutschen Unternehmen Bikeleasing-Service GmbH & Co. KG. Daher wird in weiten Teilen auf die Serverinfrastruktur des Mutterkonzerns zurückgegriffen. Für die Datenspeicherung bzw. Datenverarbeitung im Bereich der personenbezogenen Daten werden vorrangig Cloud-Lösungen genutzt.

Zum einen die Produkte des Anbieters „Microsoft Ireland Operations Limited", hier insbesondere:

- Microsoft Dynamics 365 for Sales Enterprise Online
- Microsoft SharePoint Enterprise Online
- Microsoft Exchange Enterprise Online

Des Weiteren werden Produkte des Anbieters „Amazon Web Services" (AWS) aus Irland verwendet. AWS stellt die IT-Infrastruktur für die Bikeleasing-Webseite, das Bikeleasing-Portal und die Middleware-Lösung zur Verfügung, hier insbesondere:

- Relational Database Service
- AWS EC2
- ElastiCache
- Elastic Load Balancing
- S3

Beide Dienstleister haben mit Zertifizierung nach ISO/IEC 27018 die Anforderungen an die datenschutztechnischen Anforderungen umgesetzt.

Neben der Cloudspeicherung sind am Standort Uslar und Vellmar der Bikeleasing-Service GmbH & Co. KG in einem geringeren Umfang Daten gespeichert. An den anderen Standorten werden keine Daten vor Ort gespeichert.

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

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

a. Serverseitig getroffene Zutrittskontrollmaßnahmen

01.01	Eigene Daten / Kundendaten werden auf lokalen Servern gespeichert	☐
01.02	Die Speicherung der Daten erfolgt ausschließlich lokal auf den Clients (Endgeräte)	☐
01.03	Eigene Daten / Kundendaten werden (ggf. zusätzlich) in einer Cloud gespeichert.	☒
	01.04 ☒ Microsoft ☐ Google ☒ AWS ☐	
01.05	Eigene Daten / Kundendaten werden im externen Rechenzentrum gespeichert (eigene virtuelle Server)	☐

b. Clientseitige/allgemeine getroffene Zutrittskontrollmaßnahmen

01.06	Das Bürogebäude ist teilweise / vollständig (Unzutreffendes streichen) umfriedet	☐
01.07	Ständig besetzter Empfangsbereich	☒
01.08	Elektronische / Manuelle Besucherregistrierung	☐
01.09	Büroräume haben ein elektronisches Schließsystem	☒
01.10	Büroräume haben mechanische Sicherheitsschlösser ☒	
01.11	Dokumentation der Schlüssel / Chips / Karten	☒
01.12	Bürogebäude ist videoüberwacht	☒
01.13	Bürogebäude am Standort Innsbruck ist alarmgesichert ☒	
01.14	Sorgfalt bei Auswahl des Reinigungspersonals	☒
01.15	Externer Wachdienst	☐
01.16	Biometrische Zugangssperren (z.B. Fingerscan)	☐
01.17	Persönliche Begleitung der Besucher	☒
01.18	Klingelanlage mit Kamera	☐
01.19	Lichtschranken / Bewegungsmelder sind vorhanden	☐

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

02.01	Zugangsschutz bei der EDV mit Benutzername und Passwort	☒
02.02	Eigenständiger ADMIN-Account für die Konfiguration	☒
02.03	Verbindliche Passwortparameter für die Mitarbeiterinnen und Mitarbeiter	☒
02.04	IT-System zwingt zur Einhaltung der Passwort- Vorgaben	☒
02.05	Automatische passwortgeschützte Bildschirmsperre nach spätestens 10 Min.	☒
02.06	Verbindliche Vorgaben zum manuellen Sperren des Clients	☒
02.07	Umgehende Änderung des Passwortes bei Verlust, Vergessen, Ausspähen	☒
02.08	Begrenzung von Anmeldeversuchen, danach Sperrung des Rechners	☒
02.09	Passwortgesicherte und verschlüsselte Fernzugänge	☒

02.10 Hardware-Firewall mit regelmäßiger Aktualisierung ☒
02.11 Software-Firewall mit regelmäßiger Aktualisierung ☒
02.12 Virenschutz bei Server und Clients ☒
02.13 Mobile-Device-Management zur zentralen Überwachung der mobilen Endgeräte ☒
02.14 Datenschutzkonzept / Richtlinien / Anweisungen für ein datenschutzkonformes Arbeiten ☒
02.15 Zwei-Faktor-Autorisierungsmethoden (2FA) sind ergänzend vorhanden ☒

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

03.01 Bedarfsgerechte Rechtevergabe bei Mitarbeitern ☒
03.02 Protokollierung der Zugriffe auf Daten ☒
03.03 Datenschutzkonforme Entsorgung bei externen Dienstleistern ☒
03.04 Datenschutzkonforme Vernichtung durch eigenen Shredder
(min. Schutzklasse 2, Sicherheitsstufe 3) ☐
03.05 Mobile Endgeräte (Notebook, Handy, Tablet) sind verschlüsselt ☒
03.06 Verschlüsselte Speichermedien (bspw. USB-Sticks) werden im Bedarfsfall genutzt ☐
03.07 Berechtigungskonzepte im Rahmen einer Dokumentation sind vorhanden ☒

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

04.01 Eingesetzte Systeme sind mandantenfähig (Kundentrennung) ☒
04.02 Unterschiedliche Zugriffsrechte je nach Funktion im Unternehmen ☒
04.03 Berechtigungskonzepte im Rahmen einer Dokumentation sind vorhanden ☒

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

Schutzmaßnahme ist für die Verarbeitung notwendig ☒

05.01 Testsysteme (sofern vorhanden) verarbeiten keine Echtdaten ☒
05.02 Anonymisierung/Pseudonymisierung von personenbezogenen Daten ☒

B. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

6. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

06.01	Möglichkeit zur Nutzung eines E-Mail-Zertifikates (bspw. S/Mime) zur Verschlüsselung von Mails	☒
06.02	Mobile Endgeräte sind per PIN / Passwort geschützt und verschlüsselt	☒
06.03	Nutzung eines Virtual-Private-Network (VPN) für den Zugriff auf Daten	☒
06.04	Nutzung von sicheren Transportbehältern, sofern notwendig	☐
06.05	Nutzung von datenschutzkonformen Cloud-Speichern zum Austausch von Daten	☐
06.06	Signierte E-Mails zur Sicherstellung des korrekten Absenders bei ausgewählten Personen	☒
06.07	Weitergabe der personenbezogenen Daten in anonymisierter / pseudonymisierter Form	☐
06.08	Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen, sofern Bedarf vorhanden	☐
06.09	Nutzung von verschlüsselten Verbindungen (WLAN, SSL)	☐

7. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

07.01	Protokollierung der Zugriffe auf Daten (bspw. bei einem Dokumentenmanagementsystem)	☒
07.02	Protokollierung der Systemereignisse (bspw. bei Firewall und Server)	☒
07.03	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten	☒
07.04	Klare Zuständigkeit bei Datenlöschungen	☒

C. Verfügbarkeit/Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

8. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

a. Serverseitig getroffene Zutrittskontrollmaßnahmen

08.01	Eigene Daten / Kundendaten werden auf lokalen Servern gespeichert	☐
08.02	Die Speicherung der Daten erfolgt ausschließlich lokal auf den Clients	☐
08.03	Eigene Daten / Kundendaten werden in einer Cloud gespeichert.	☒
08.04	Eigene Daten / Kundendaten werden in einem externen Rechenzentrum gespeichert (eigene virtuelle Server)	☐

b. Clientseitige/allgemeine getroffene Zutrittskontrollmaßnahmen

08.12	IT-Systeme sind mit Virenschutz und Software-Firewall geschützt	☒
08.13	Schriftliches Notfallkonzept	☒

08.14	Zügige Wiederherstellbarkeit des laufenden Betriebes ist möglich	☒
08.15	Schriftliches Backup-Konzept	☒
08.16	Funktionalität der Wiederherstellung von Backups wird regelmäßig getestet	☒
08.17	Datensicherungen erfolgen regelmäßig	☒
08.18	Datensicherungen sind verschlüsselt	☒
08.19	Datensicherungen werden extern aufbewahrt (getrennter Brandabschnitt)	☒
08.20	Regelmäßige USV-Tests (USV=Sicherungsbatterie für Serversysteme)	☒

D. Verfahren zur regelmäßigen Überprüfung und Bewertung
(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

9. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

09.01	Unternehmen hat einen Datenschutzbeauftragten (DSB) benannt	☒
09.02	Mitarbeiter werden schriftlich auf die Vertraulichkeit verpflichtet	☒
09.03	Bei Dienstleistern wird auf deren Qualifikation geachtet	☒
09.04	Notwendige Auftragsverarbeitungsvereinbarung werden geschlossen	☒
09.05	Regelmäßige Prüfung der Technischen und organisatorischen Maßnahmen des Auftragsverarbeiters	☒
09.06	Regelmäßige Überprüfung der eigenen Technischen + Organisatorischen Maßnahmen	☒
09.07	Interner / externer Informationssicherheitsbeauftragter	☒

10. Datenschutz-Management

Zentrale Verwaltung, Nachvollziehbarkeit und Protokollierung des aktuellen Datenschutzniveaus im Unternehmen

10.01	Zentrale und strukturierte Ablage aller datenschutzrechtlichen Dokumente	☒
10.02	Nutzung einer Datenschutzmanagementsoftware	☐
10.03	Bedarfsgerechte Durchführung von Datenschutz-Folgenabschätzung (DSFA)	☒
10.04	Umsetzung der Informationspflicht gem. Art. 13/14 DSGVO	☒
10.05	Regelmäßiger Austausch zwischen Unternehmen und Datenschutzbeauftragten	☒
10.06	Regelmäßige Prüfung des Verarbeitungsverzeichnisses und des Datenschutzkonzeptes	☒
10.07	Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)	☒
10.08	Protokollierung aller Maßnahmen und Entscheidungen	☒
10.09	Sicherheitszertifizierung nach ISO 27001	☐

11. Incident-Response-Management

Umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT/Datenschutz-Bereichen berücksichtigen.

11.01	Unterstützung durch Sicherheitssoftware (Firewall, Spamfilter, Virenschutz)	☒
11.02	Meldewege und Meldeprozesse bei Sicherheitsvorfällen und Datenpannen sind bekannt	☒
11.03	Einbindung des Datenschutzbeauftragten bei Sicherheitsvorfällen und Datenpannen	☒
11.04	Dokumentation von Sicherheitsvorfällen und Datenpannen	☒

12. Datenschutzfreundliche Voreinstellungen

(Art. 25 Abs. 2 DS-GVO)

Einstellungen von Soft- und Hardware vor Nutzung und Herausgabe an Benutzer bzw. Kunden

12.01	Beachtung von Datenschutz bei der App-Entwicklung und Softwareprogrammierung	☒
12.02	Beachtung von Datenschutz bei der Konfiguration von Systemen (Software + Hardware)	☒
12.03	Minimalprinzip bei der Erfassung personenbezogener Daten	☒
12.04	Pseudonymisierung / Anonymisierung von personenbezogenen Daten	☐
12.05	Größtmögliche Transparenz bei der Verarbeitung personenbezogener Daten	☒

13. Einsatz von Künstlicher Intelligenz (KI)

(Art. 25 Abs. 2 DS-GVO)

Maßnahmen, die das Ziel haben, dass die künstliche Intelligenz (KI) datenschutzkonform eingesetzt bzw. genutzt wird.

KI ist bei <u>uns</u> aktiv im Einsatz ☒

KI verarbeitet personenbezogene Daten ☐

13.01	Verwendung von anonymisierten Datensätzen für das Training von KI-Modellen	☐
13.02	Transparenz der Entscheidungen, die durch KI-Systeme getroffen werden	☐
13.03	Protokollierung der Datenquellen und Verarbeitungsschritte innerhalb der KI-Modelle	☐
13.04	Maßnahmen zur Vermeidung + Erkennung von Fehleinschätzungen in der KI	☐
13.05	Monitoring Überwachung der Zugriffe	☐
13.06	Regelmäßige Überprüfung bzgl. der Datenschutzkonformität	☒
13.07	Regelmäßige Schulungen für Mitarbeiter zum Thema KI	☒
13.08	Regelmäßige Sicherheitsupdates der KI-Systeme	☒
13.09	Regelmäßige Audits der KI-Systeme auf Sicherheits- und Datenschutzaspekte	☒
13.10	Prüfung bzgl. kontinuierlicher Verbesserung der KI-Modelle und Sicherheitsmaßnahmen	☒

KI ist bei <u>unseren Unterauftragnehmern</u> aktiv im Einsatz ☒

☒ Microsoft ☐ Google ☐ AWS ☐ .....

(Diese verarbeiten personenbezogene Daten unserer Kunden.)

13.11	Bei der Verarbeitung von personenbezogenen Daten werden diese anonymisiert	☒
13.12	Auftragsverarbeitungsvereinbarung (AVV/DPA) mit dem Dienstleister sind vorhanden	☒
13.13	Regemäßige Prüfung und Anpassung der datenschutzrechtlichen Einstellungen	☒
13.14	Dienstleister ist ISO-zertifiziert	☒

14. Mobiles Office/Home-Office

Unsere Mitarbeiterinnen und Mitarbeiter unterstützen aus dem mobilen Office bzw. dem Home-Office.

14.01	Alle Daten werden auf Serverstrukturen im Unternehmen gespeichert	☒
14.02	Alle Daten werden auf Serverstrukturen beim Auftragsverarbeiter (Cloud/Rechenzentrum) gespeichert	☒
14.03	Ergänzende Richtlinien und Dokumente beschreiben den Umgang mit Daten bzw. den Schutz von Daten	☒

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung

zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

BLS Bikeleasing-Service Österreich GmbH

Exlgasse 24, A - 6020 Innsbruck

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Europäischen Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer (Beschreibung der Unterstützung):

Unterstützung im Bereich IT, Personal und Marketing/Web

☐ Der Gegenstand des Vertrags ergibt sich aus der Leistungsvereinbarung/ dem Vertrag.

(2) Dauer

☒ Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

☐ Der Auftrag ist befristet erteilt. Er beginnt am ..... und endet am .....

(3) Diese Vereinbarung gilt so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

3. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

☒ Bereitstellung und Betrieb inkl. Wartung der Dokumentenablagestruktur

☒ IT-Administration und Support

☒ Unterstützung im Gesamtbereich Personal

☒ Unterstützung im Gesamtbereich Marketing/Web

☒ Unterstützung im Bereich der Benefitverteilung / Benefitübersicht

☒ Unterstützung im Bereich der Gutscheinausstellung

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

☒ Daten im Rahmen des Leasing-Angebotes

☒ Daten im Rahmen der Personalverwaltung

☒ Stammdaten von Kunden und Mitarbeitern

☒ Kommunikationsdaten (z.B. E-Mail)

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☒ Vertragsabrechnungs- und Zahlungsdaten

☒ Server-Logdateien

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Beschäftigte des Auftraggebers

☒ Kunden des Auftraggebers

4. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten, insbesondere hinsichtlich der konkreten Auftragsdurchführung, und übergibt dem Auftraggeber die Dokumentation zur Prüfung. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Soweit eine Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen 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.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.
(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.
(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

6. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technischer und organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

7. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
Als Datenschutzbeauftragter ist beim Auftragnehmer bestellt
Herr RA Wolfgang Stenzel, LL.M.
Keesgasse 3, 8010 Graz

b) Telefon: +43 (0) 316 42 00 04 Mail: datenschutz@bikeleasing.at Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dabei berücksichtigt der Auftragnehmer auch, dass ihm vom Auftraggeber Daten zur Verfügung gestellt werden, die ggf. einem besonderen Berufsgeheimnisschutz unterfallen.

c) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO].

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
f) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. 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.
g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
j) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber unterstützt ihn der Auftragnehmer.
k) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
l) Die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
m) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.
n) Sofern der Auftraggeber ein Berufsgeheimnisträger ist, ist dem Auftragnehmer bekannt, dass Verstöße im Rahmen des Berufsgeheimnisses nach § 203 StGB strafbewährt sind.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

8. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftrag-nehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaß-nahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

☐ Eine Unterbeauftragung ist unzulässig.

☒ Der Auftraggeber stimmt der Beauftragung der aufgelisteten Unterauftragnehmer gem. Anlage zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

(3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit (min. 4 Wochen) vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technischen und organisatorischen Maßnahmen beim Unter-auftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

(6) sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

9. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO.

☐ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

☒ Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet primär in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Aufgrund von technischem Routing von Daten bzw. der Zugriffsmöglichkeit durch den jeweiligen Gesetzgebern zu Kontroll- bzw. Überwachungszwecken kann ein Zugriff nicht ausgeschlossen werden. Grundlage dieser Verarbeitungen sind EU-Standardvertragsklauseln.

☐ Der Auftraggeber gestattet eine direkte Datenübermittlung in ein Drittland. Hierzu werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dienstleister/Unterauftragnehmer in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

(3) Sollten personenbezogene Daten Betroffener in Länder außerhalb der EU bzw. des EWR übermittelt werden, so erfolgt dies nur bei Bestehen eines Angemessenheitsbeschlusse der Europäischen Kommission (Art. 45 Abs. 1 DSGVO) oder dem Vorliegen geeigneter Garantien (Art. 46 DSGVO) oder unter den Voraussetzungen des Art. 49 DSGVO) für Ausnahmen in bestimmten Fällen.

(4) Jede Verlagerung in ein Drittland außerhalb der EU bzw. dem EWR oder einem Land ohne Bestehen eines Angemessenheitsbeschlusses der Europäischen Kommission bedarf der vorherigen Zustimmung des Auftraggebers.

10. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Kontrollen durch den Auftraggeber werden durch den Auftragnehmer in der Regel nicht in Rechnung gestellt. Sofern bei einer Vorort-Prüfung der Wunsch des Auftraggebers bzw. der Bedarf besteht, dass weiteres Fachpersonal, neben dem Datenschutzkoordinator, zugegen sein soll bzw. muss, kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Die betreffenden Kostennoten werden dann vorab mitgeteilt.

(5) Überprüfungen und Inspektionen durch den Auftraggeber im Geschäftsbetrieb des Auftragnehmers sind grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle des mobilen Arbeitsplatzes von Beschäftigten durch den Auftragnehmer zu ermöglichen.

(7) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

11. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu

einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Entstehende Mehraufwände des Auftragnehmers infolge der Weisung trägt der Auftraggeber, sofern sich nachträglich herausstellt, dass die Weisung tatsächlich rechtswidrig war. Die Verantwortung für die getroffene Entscheidung liegt ausschließlich beim Auftraggeber. Besteht der Auftraggeber auf der Ausführung der Weisung, obwohl diese nach Einschätzung des Auftragnehmers weiterhin rechtswidrig ist, steht es dem Auftragnehmer frei eine Entscheidung der zuständigen Aufsichtsbehörde einzuholen, oder die Verarbeitung abzulehnen.

12. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13. Haftung

(1) Art. 82 DSGVO kommt zur Anwendung

14. „Mobiles Arbeiten"-Regelung

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von diesen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten, für das mobile Arbeiten relevanten, technischen und organisatorischen Maßnahmen auch bei der Nutzung von mobilen Arbeitsplätzen der Beschäftigten des Auftragnehmers gewährleistet ist.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere am Ort des jeweiligen mobilen Arbeitsplatzes befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag an mobilen Arbeitsplätzen durch den Auftraggeber möglich ist.
(5) Sofern auch bei Unterauftragnehmern Beschäftigte im „Mobilen-Arbeiten" eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

15. Schlussbestimmungen

(1) Die Vertragsparteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Vertragspartei vertraulich zu behandeln. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung die jeweilige Vertragspartei ein berechtigtes Interesse hat. Eine Geheimhaltungspflicht besteht auch nach Beendigung dieses Vertrags fort.
(2) Sofern eine Vertragspartei weiteren Geheimnisschutzregeln unterliegt und sie dies der anderen Vertragspartei zu Vertragsbeginn schriftlich mitteilt, ist auch diese Vertragspartei verpflichtet, die Geheimnisschutzregeln zu beachten.
(3) Für Vertragsänderungen und Nebenabreden ist die Schriftform erforderlich.
(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

16. Unterschriften

Ort, Datum Innsbruck, 29.10.2025	Ort, Datum Innsbruck, 29.10.2025
Auftraggeber	Auftragnehmer

Anlage Unterauftragnehmer

☐ Keine Unterauftragnehmer vorhanden

Unterauftragnehmer	Anschrift	Leistung
Ascendit GmbH	Wittland 2-4 24109 Kiel	Bearbeitung und Editierung von CRM
BLS Versicherungs GmbH & Co. KG	Bewdley-Platz 20-22 34246 Vellmar	Unterstützung im Rahmen der Kundenbetreuung
Microsoft Irland	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Hosting und Bereitstellung von Cloud-Produkten
Blackbit	Ernst-Ruhstrat-Straße 6 37079 Göttingen	Programmierung Portal und App
Signaturit	Avila 26. Street 08005 Barcelona	Digitale Signatur
Amazon AWS	Eschborner Landstrasse 100 60489 Frankfurt am Main	Hosting und Bereitstellung
Microsoft Corporation	Microsoft Deutschland GmbH Walter-Gropius-Strasse 5 80807 München Germany	Login und Authentifizierung
Google Ireland Limited	Gordon House, Barrow Street Dublin 4 Irland	Verwaltung von PushBenachrichtigungen Standortservice Google Maps
Tiffinger und Thiel GmbH	Äußere Münchener Straße 81 84036 Landshut Germany	Unterstützung bei der Weiterentwicklung der ProbonioPlattform
Zendesk GmbH	Zendesk GmbH c/o TaylorWessing Neue Schönhauser Str. 3-5 10178 Berlin Germany	Verwaltung von Support- und Feedbackanfragen
Kombo Technologies GmbH	Rosenthaler Str. 72A Berlin 10119	Integration externer HR-Systeme
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxemburg	Rechenzentrum Hosting der Probonio Plattform und Datenbank Künstliche Intelligenz zur Unterstützung der Einzelbelegkontrolle
Probonio GmbH	Äußere Münchener Straße 81 84036 Landshut	Benefit Verwaltung