Vereinbarung zum Datenschutz zur Auftragsverarbeitung

02.11.2021

Inhaltsverzeichnis

Inhalt

1 Einführung

Der **Auftragnehmer**

BLP Digital AG
Technoparkstrasse 1
8005 Zürich
Schweiz

verarbeitet personenbezogene Daten für den **Auftraggeber**

Name Unternehmen
Strasse
PLZ / Ort
Schweiz

2 Präambel

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – 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.

3 Gegenstand der Vereinbarung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in **Anlage 1** näher definiert.

(2) Die vom Auftrag umfassten Kategorien betroffener Personen und die Arten der Datenkategorien sind in **Anlage 2** aufgeführt.

(3) Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung (siehe **Anlage 1**).

(4) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoss des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

(5) Änderungen des Verarbeitungsgegenstandes, Verarbeitungsumfanges sowie Verfahrensänderungen sind schriftlich zu vereinbaren.

(6) Die Verarbeitung und Nutzung der Daten findet in der Schweiz als anerkanntes sicheres Drittland statt, einem Drittland, in dem die Anforderungen an Unterauftragsnehmer nachweislich per technischer und organisatorischer Massnahmen (siehe **Anlage 5**) gemäss den DSGVO-Anforderungen dokumentiert, umgesetzt und überwacht sind.

(7) Der Vertrag beginnt mit der Unterzeichnung beider Vertragsparteien.

4 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschliesslich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. Der Auftragnehmer teil dem Auftraggeber in jedem Fall mit, vor dem Zugriff, wenn eine öffentliche Institution Zugriff auf seine Daten ausüben will, unabhängig der rechtlichen Grundlage, die dies ermöglicht. Der Begriff "Zugriff" umfasst auch die Übermittlung der Daten im Sinne der nächsten Ziffer 2. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschliesslich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für die vereinbarten Vertragszwecke. Eine Verarbeitung oder Nutzung ohne Kenntnis des Auftraggebers oder zu eigenen Zwecken des Auftragnehmers ist nicht erlaubt. Eine Übermittlung an Dritte ist nicht gestattet, sofern nicht gesetzliche Vorgaben den Auftragnehmer hierzu verpflichten. Kopien oder Duplikate 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.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemässen Verarbeitung von personenbezogenen Daten die vertragsmässige Abwicklung aller vereinbarten Massnahmen zu. Insbesondere sichert der Auftragnehmer in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Massnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Mass gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen, die für die Sicherheit der Daten erheblich sind, in der Organisation der Datenverarbeitung im Auftrag vorab mit dem Auftraggeber abstimmen.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstösst. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Massnahmen ist Bestandteil dieses Vertrages. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Massnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit

dem Auftraggeber abstimmen. Massnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Massnahmen anfordern.

(7) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten in **Anlage 3** mitteilen. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(8) Der Auftragnehmer verpflichtet sich, soweit rechtlich und tatsächlich möglich, den Verantwortlichen auch mit geeigneten technischen und organisatorischen Massnahmen bei der Beantwortung von Anträgen zu unterstützen, die Betroffene zur Ausübung ihrer Rechte nach Art. 12-22 DSGVO an den Auftraggeber stellen. Dies betrifft insbesondere das Auskunftsrecht der Betroffenen (Art. 15 DSGVO), das Recht auf Berichtigung unrichtiger personenbezogener Daten, das Recht der Betroffenen auf Löschung ihrer personenbezogenen Daten (Art. 17 DSGVO) sowie das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Der Auftragnehmer darf Daten nur auf dokumentierte Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Er wird ferner keinerlei Auskunft über personenbezogene Daten an Dritte, aber auch nicht an den Betroffenen selbst erteilen. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer darf der betroffenen Person in diesem Zusammenhang die Kontaktdaten des Verantwortlichen mitteilen.

(9) Der Auftragnehmer gewährleistet, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie massgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet hat, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Dies gilt insbesondere in den Fällen, in denen der Auftraggeber zur Einhaltung der Schweigepflicht aus § 203 StGB verpflichtet ist. Der Auftraggeber wird dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitteilen.

(10) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoss gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(11) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO im Falle einer Datenschutzverletzung bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich nach Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Massnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(12) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

(13) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten, die den Anforderungen des Art. 30 Abs. 2 DSGVO genügt. Hinsichtlich des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers hat der Auftragnehmer den Auftraggeber auf Anforderung in dem ihm möglichen Umfang zu unterstützen.

(14) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung zu stellen. Er erteilt auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.

(15) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind.

(16) Der Auftragnehmer verpflichtet sich zur Durchführung regelmässiger Kontrollen im Hinblick auf die Vertragsausführung bzw. -erfüllung, der Einhaltung und ggf. notwendiger Anpassungen von Regelungen und Massnahmen zur Durchführung des Auftrags. Dies umfasst insbesondere auch regelmässige und anlassbezogene Kontrollen der Wirksamkeit vereinbarter technischer und organisatorischer Massnahmen zur Sicherheit personenbezogener Daten.

5 Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte nach den Art. 12 bis 22 DSGVO allein verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen der beschriebenen Pflichten

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 4** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber

ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen. Entsprechend können Ansprechpartner des Auftragnehmers hier benannt werden, an die Weisungen zu richten sind.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmässigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

6 Rechte des Auftraggebers / Kontrollen

(1) Der Umgang mit den personenbezogenen Daten erfolgt ausschliesslich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen

(2) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(3) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(4) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(5) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 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.

(6) Der Auftragnehmer ist verpflichtet, im Falle von Massnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Massnahmen vom Auftragnehmer zu informieren.

7 Weitere Auftragsverarbeiter (Unterauftragnehmer)

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers in Textform zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmässig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Massnahmen zum

Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäss Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schliessen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmassnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Massnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Datenträgervernichtung sowie Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Datenträgervernichtung, Wartung und Pflege solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogene Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

8 Vertraulichkeit

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. deren Kenntnis er erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie massgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten

tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

(4) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(5) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind sowie im Rahmen von gesetzlich gebotenen Offenlegungen gegenüber öffentlichen Stellen.

9 Beendigung des Vertrages

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäss DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemässe Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

10 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Massnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Diese Vereinbarung zum Datenschutz ersetzt alle zuvor getroffenen Vereinbarungen zum Datenschutz zwischen dem Auftraggeber und dem Auftragnehmer.

(3) Die Allgemeinen Geschäftsbedingungen der BLP Digital AG ergänzen diese Vereinbarung.

(4) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschliesslich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw.

Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

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

11 Gerichtsstand

Die Parteien vereinbaren über alle Rechtsbeziehungen aus diesem Vertrag zur Anwendung des Rechts der Schweizerischen Eidgenossenschaft. Für alle Streitigkeiten, die sich im Rahmen der Durchführung dieses Vertragsverhältnisses ergeben, wird Zürich (Schweiz) als ausschliesslicher Gerichtsstand vereinbart.

Name des Unternehmens		**BLP Digital AG**	
……..	……	……..	……
Datum	Unterschrift	Datum	Unterschrift

Anlage 1: Leistungsbeschreibung

Die Tätigkeiten des Auftragnehmers für den Auftraggeber im Rahmen der Auftragsdatenverarbeitung sind wie folgt festgelegt (Mehrfachnennungen sind möglich):

☐ Tätigkeiten sind der nachfolgenden **Leistungsbeschreibung(en)/Vertrag/SLA** zu entnehmen:

- ☐ Name der Vereinbarung:

- ☐ Name der Vereinbarung:
  abgeschlossen am:

- ☐ Name der Vereinbarung:
  abgeschlossen am:

☐ IT-Dienstleistungen

- ☐ Pflege und Wartung der folgenden Software-Produkte:
- ☐ Betrieb des folgenden Software-Produkts (Hosting):
- ☐ Pflege und Wartung der folgenden Hardware-Produkte:
- ☐ Bereitstellung von Online-Speicherplatz (Cloud)
- ☐ Bereitstellung von Rechenzentrums-Leistungen:
- ☐ Hotline- und Online-Support für IT-Fragestellungen (User-Help-Desk)
- ☐ Sonstige:

☐ **Weitere Beschreibungen der Leistungen soweit nicht aus SLA oder Hauptvertrag hervorgehend** (Bitte ausfüllen soweit zutreffend).

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Anlage 2: Betroffene Personen und Datenkategorien (vom Auftraggeber auszufüllen)

Der Auftragnehmer verarbeitet vertragsgemäss auch personenbezogene Daten für den Auftraggeber. Diese werden im Folgenden spezifiziert. Bedingt durch den technologischen Wandel und organisatorische Veränderungen kann sich die Zusammensetzung der Daten auch verändern.

Betroffene Personengruppen

- ☐ Mitarbeiter/Beschäftigte/Bewerber des Auftraggebers
- ☐ ehemalige Mitarbeiter/Beschäftigte des Auftraggebers (Rentner)
- ☐ Mitarbeiter von verbundenen Unternehmen des Auftraggebers
- ☐ externe Dienstleister / eigenverantwortliche Stellen (Steuerberater, Rechtsanwälte, Betriebsärzte) des Auftraggebers
- ☐ Mitarbeiter von Geschäftspartnern des Auftraggebers
- ☐ Interessenten/Bewerber des Auftraggebers
- ☐ Lieferanten des Auftraggebers
- ☐ Mitarbeiter/Kunden/Interessenten/Geschäftspartner von Kunden des Auftraggebers (bei Unterauftragsverarbeitung)

Datenkategorien

- ☐ Stamm- und Kommunikationsdaten (private Namen, Anschriften, Telefonnummern)
- ☐ Stamm- und Kommunikationsdaten (geschäftliche Anschriften, Telefonnummern,
- ☐ Funktionsbeschreibungen)
- ☐ Kosten-/Leistungsabrechnungsdaten (Reisekostenabrechnung, Betriebsrenten, Zuschläge etc.)
- ☐ Abrechnungsdaten (Lohn-/Gehaltsabrechnungen, Bankverbindungen etc.)
- ☐ Bewerbungsunterlagen (Qualifikationen, Ausbildung, Bewerbungsbilder, Zeugnisse etc.)
- ☐ Daten von BDE-Systemen (Betriebsdatenerfassung)
- ☐ Zeiterfassungsdaten
- ☐ Leistungserfassungs-/Abrechnungsdaten
- ☐ Bankverbindungen (natürlicher Personen)
- ☐ Daten der Mitarbeiter in CRM-Systemen (Vertrieb, Service-Center)
- ☐ Incident-Management-/Ticket-Systeme
- ☐ IT-Systemspezifische Daten, wie z.B. Benutzernamen, Zugriffsrechte, Nutzerprofile
- ☐ persönliche Identifikationsnummern (Mitarbeiter-ID, IP-Adresse)
- ☐ Personalaktendaten (Zeugnisse, Sozialversicherungsnummer, Beurteilungen, Protokolle)
- ☐ Personalausweisdaten (Kopien der Ausweisdokumente)
- ☐ Lichtbilder/Digitalfotos natürlicher Personen (z.B. für Mitarbeiterprofile)
- ☐ Besondere Daten der betroffenen Personen (gemäss Artikel 9 DSGVO)
    - ☐ Daten aus denen rassische / ethnische Herkunft hervorgehen
    - ☐ Daten aus denen politische Meinungen hervorgehen
    - ☐ Daten aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen (koscheres Essen)
    - ☐ Daten aus denen die Gewerkschaftszugehörigkeit hervorgeht
    - ☐ genetische Daten (vgl. Artikel 4 Nr. 13 DSGVO)
    - ☐ biometrische Daten (vgl. Artikel 4 Nr. 14 DSGVO)
    - ☐ Gesundheitsdaten (vgl. Artikel 4 Nr. 15 DSGVO) (Allergien, Ernährung, Behinderungen)
    - ☐ Daten zum Sexualleben oder zur sexuellen Orientierung
- ☐ sonstige:

Anlage 3: Betriebliche Datenschutzbeauftragte

Datenschutzbeauftragter des Auftragnehmers:

☐	Der Auftragnehmer ist gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. (Angaben zur Geschäftsführung nur dann erforderlich)	
	Ansprechpartner GF (Name Geschäftsführer)	
	Telefon	
	E-mail	
☒	Betrieblicher Datenschutzbeauftragter (Art. 37 DSGVO / § 38 BDSG)	
	Firma (bei externem DSB)	BLP Digital AG
	Anschrift	**Technoparkstrasse 1, 8005 Zürich, Schweiz**
	Name	**Tim Beck**
	Telefon	**0041754131921**
	E-mail	**tim.beck@blp-digital.com**

Datenschutzbeauftragter des Auftraggebers:

Name: Max Mustermann
Anschrift: Musterstrasse 123, 8005 Zürich, Schweiz
Tel.-Nr.: (0041) XX XX XXX
E-Mail: max.mustermann@muster.ch

Anlage 4: Liste der Weisungsberechtigten und Ansprechpartner

Weisungsberechtigte des Verantwortlichen (Auftraggeber)	
Name	
Funktion	
Kontakt	
Name	
Funktion	
Kontakt	

Ansprechpartner des Auftragnehmers (Projektverantwortliche beim Auftragsverarbeiter)	
Name	Tim Beck
Funktion	CEO
Kontakt	Technoparkstrasse 1, 8005 Zürich, Schweiz / tim.beck@blp-digital.com
Name	Sven Beck
Funktion	CTO
Kontakt	Technoparkstrasse 1, 8005 Zürich, Schweiz / sven.beck@blp-digital.com

Anlage 5: Technische und Organisatorische Massnahmen

1 Versionierung und Historie

Version	Datum	Erstellt	Geprüft
1.2	02.11.2021	Tim Beck	Sven Beck
1.1	05.07.2020	Tim Beck	Sven Beck
1.0	20.10.2019	Sven Beck	Tim Beck

2 Einführung

Die BLP Digital AG hat umfassende technische und organisatorische Massnahmen ergriffen, um die Anforderungen an Datenschutz und Datensicherheit gemäss Artikel 32 der DSGVO zu erfüllen. Im Folgenden werden die etablierten Massnahmen im Prinzip beschrieben. Dieses Dokument ist Teil der Dokumentation des firmeninternen Datenschutzmanagementsystems. Dieses Dokument gilt für die informationsverarbeitenden Systeme und Netzwerke, Dokumente und Informationen der BLP Digital AG, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden. Diese Version des Dokumentes ersetzt alle früheren Versionen und Ausgaben. Sollten vertragliche oder gesetzliche Festlegungen dieses Dokument oder Teile hiervon berühren, haben diese in jedem Fall Vorrang.

3 Zutrittskontrolle

Folgende Massnahmen wurden ergriffen, um ausschliesslich Befugten den Zutritt in Büro- und Geschäftsräume zu ermöglichen:

- Alle Zugänge zu Büro- und Geschäftsräumen sind grundsätzlich geschlossen und nur per Firmenschlüssel zugänglich.
- Die Vergabe von Firmenschlüsseln erfolgt nach einem definierten Prozess, der sowohl zu Beginn als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug regelt und dokumentiert.
- Besucher dürfen sich ausschliesslich in Begleitung von autorisierten Mitarbeitern in den Büro- und Geschäftsräumen bewegen.

4 Zugangs- und Zugriffskontrolle

Folgende Massnahmen wurden ergriffen, um ausschliesslich Befugten den Zugang zu den Datenverarbeitungssystemen zu ermöglichen:

- Jeder Mitarbeiter unterzeichnet vor Antritt seiner Tätigkeit eine Vertraulichkeitserklärung.
- Jeder Mitarbeiter wird regelmässig im Umgang mit personenbezogen Daten geschult.
- Alle Systeme sind durch eine Zugangskontrolle geschützt.
- Jedem Mitarbeiter werden individuelle Zugangsberechtigungen ausschliesslich durch autorisierte Administratoren zur Verfügung gestellt.
- Berechtigungen für Datenverarbeitungssysteme werden nach dem „Minimalprinzip“ vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten verarbeiten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.
- Passwortvorgaben beinhalten Vorgaben, die sich an den Standards des deutschen Bundesamtes für Sicherheit in der Informationstechnik orientieren, wie zum Beispiel Passwortlänge, Zeichenmischung, Ausschluss von Trivialpasswörtern, Passworthistorie, definierte Verfahren bei wiederholt fehlgeschlagenem Login-Versuch, etc.
- Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

- Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für den Auftraggeber im Einsatz sind, sind durch Firewalls geschützt, die gewartet und mit aktuellen Updates und Patches versorgt werden.
- Von der Firma verwendete Hard- und Software wird ausschliesslich für firmeninterne Tätigkeiten eingesetzt. Der Einsatz für private Zwecke ist untersagt.
- Die Installation von Software ist ausschliesslich in Absprache mit autorisierten Administratoren zulässig.
- Die Vernichtung von Datenträgern und Papier erfolgt nach den Anforderungen der DIN 66399.

5 Datentrennung und Eingabekontrolle

Folgende Massnahmen wurden ergriffen, um die für verschiedene Zwecke und/oder Kunden erhobenen Daten getrennt verarbeiten zu können:

- Eine Funktionstrennung, die Differenzierung der Berechtigungen und eine angemessene Gestaltung der Vergabeverfahren gewährleisten die Trennung der verschiedenen Datenbestände.
- Implementierte differenzierte Zugriffsberechtigungen für verschiedene Benutzer entsprechend ihren Rollen und Verantwortlichkeiten.
- Eine Zugriffsberechtigungsmatrix wird verwendet, um sicherzustellen, dass verschiedene Benutzer nur auf für ihre Aufgaben erforderliche Daten zugreifen können.
- Der Benutzername des verarbeitenden Mitarbeiters und der konkrete Zeitpunkt der Dateneingabe werden für die Verarbeitungen von personenbezogenen Daten in den Systemen protokolliert.

6 Pseudonymisierung und Verschlüsselung

Folgende Massnahmen wurden ergriffen, um die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten sicherzustellen:

- Die Übertragung von personenbezogenen Daten wird durch aktuelle Sicherheitsprotokolle mit starken Verschlüsselungsalgorithmen (mindestens 256-Bit- Standard) und Schlüsseln geschützt.

7 Verfügbarkeit und Belastbarkeit

Folgende Massnahmen wurden ergriffen, um die Verfügbarkeit und Belastbarkeit der Datenverarbeitungsysteme sicherzustellen:

- Alle Daten, einschliesslich personenbezogener Daten, werden regelmässig gesichert, um sicherzustellen, dass die Daten auch im Notfall verfügbar sind.
- Ein Datensicherungskonzept ist vorhanden und beinhaltet das erfolgreiche Testen der Wiederherstellung von Daten.
- Daten-Risikobewertungen werden jährlich durchgeführt und es existiert ein Risiko- und Reaktionsplan.
- Kritische Systeme sind redundant ausgelegt.

8 Auftragskontrolle

Folgende Massnahmen wurden ergriffen, um die Anforderungen der DSGVO bei Unterauftragnehmern durchgängig zu gewährleisten:

- Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit dem Auftraggeber abgestimmt ist.
- Mit jedem Unterauftragnehmer ist ein Auftragsdatenverarbeitungsvertrag abgeschlossen.
- Unterauftragnehmer werden regelmässig im Hinblick auf die Vertragsausführung, Einhaltung und ggf. notwendigen Anpassungen von Regelungen und Massnahmen zur Durchführung des Auftrags kontrolliert.

9 Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen

Folgende Massnahmen wurden ergriffen, um einen ordnungsgemässen Prozess für die regelmässige Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Massnahmen sicherzustellen:

- Eine jährliche Managementbewertung wird für die Umsetzung, Feststellung und Verbesserung der technischen und organisatorischen Massnahmen durchgeführt.
- Regelmässige und unregelmässige Audits werden für die Gewährleistung der technischen und organisatorischen Massnahmen durchgeführt.
- Mindestens jährliche Schulungsprogramme werden für alle Mitarbeiter durchgeführt, um sicherzustellen, dass die firmeninternen Richtlinien, inklusive dieser technischen und organisatorischen Massnahmen, bekannt sind und eingehalten werden.