BetriebPlus - Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

Stand: 13. August 2026 · **Version:** 3.1

> Diese Fassung ersetzt für neue Vertragsschlüsse bzw. die öffentliche Bereitstellung die Fassung vom 11.08.2026.

Vertragsparteien

AUFTRAGGEBER	AUFTRAGNEHMER
Name / Firma	**Tobias Weirich, handelnd unter „BetriebPlus“** Am Pfingstbruch 8 34471 Volkmarsen Deutschland Datenschutz: datenschutz@betriebplus.com Support: support@betriebplus.com
Rechtsform	
Anschrift	
Vertreten durch	
E-Mail / Datenschutzkontakt	
Kundennummer, soweit vorhanden	

Auftraggeber und Auftragnehmer werden gemeinsam „Parteien“ genannt.

1. Gegenstand, Geltungsbereich und Rangfolge

1.1 Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch BetriebPlus im Auftrag des Auftraggebers im Zusammenhang mit der Bereitstellung und Nutzung der BetriebPlus-Web-App.

1.2 Er gilt nur, soweit BetriebPlus personenbezogene Daten als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet. Verarbeitungen, bei denen BetriebPlus selbst Zwecke und Mittel bestimmt, sind nicht Gegenstand dieses AVV und werden in der Datenschutzerklärung beschrieben.

1.3 Die Art der Leistung ergibt sich aus Hauptvertrag und Leistungsbeschreibung. Die datenschutzrechtliche Verarbeitung ist in Anlage 1 konkretisiert.

1.4 Für Gegenstände der Auftragsverarbeitung nach Art. 28 DSGVO geht dieser AVV allen übrigen Vertragsunterlagen vor. Echte Individualabreden bleiben nach § 305b BGB vorrangig; eine Abweichung von diesem AVV gilt jedoch nur, wenn sie ausdrücklich als Änderung oder Ergänzung des AVV vereinbart ist.

1.5 Dieser AVV wird vor Beginn der Auftragsverarbeitung in einer Form abgeschlossen, die seinen Inhalt und die vereinbarte Fassung dauerhaft dokumentiert. Zulässig sind insbesondere eine gesonderte handschriftliche oder elektronische Unterzeichnung, eine dokumentierte elektronische Annahme oder die ausdrückliche Einbeziehung einer eindeutig bezeichneten AVV-Fassung in Angebot, Auftragsbestätigung oder Freischaltungsbestätigung, sofern der AVV dem Auftraggeber zuvor in speicher-und reproduzierbarer Form bereitgestellt wurde. BetriebPlus dokumentiert den Abschluss und die einbezogene Fassung. Vor Wirksamwerden des AVV erfolgt keine Verarbeitung personenbezogener Echtdaten im Auftrag.

2. Rollen der Parteien

2.1 Der Auftraggeber ist für die von ihm bestimmten Verarbeitungen regelmäßig Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Er entscheidet insbesondere über Zwecke, Rechtsgrundlagen, Nutzerkreis, fachliche Aufbewahrungsfristen und zulässige Nutzung.

2.2 BetriebPlus verarbeitet die in Anlage 1 beschriebenen personenbezogenen Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers, soweit nicht Unionsrecht oder das Recht eines Mitgliedstaats eine Verarbeitung verlangt.

2.3 Eine gemeinsame Verantwortlichkeit wird nicht vereinbart. Ergibt sich für einen konkreten Verarbeitungsvorgang tatsächlich eine andere Rollenverteilung, stimmen die Parteien vor Fortsetzung dieser Verarbeitung die erforderliche rechtliche Regelung ab.

2.4 Handelt der Auftraggeber seinerseits als Auftragsverarbeiter für einen Dritten, sichert er zu, zur Beauftragung von BetriebPlus als weiterem Auftragsverarbeiter berechtigt zu sein. Art. 28 Abs. 4 DSGVO bleibt unberührt.

3. Dauer, Art und Zweck der Verarbeitung

3.1 Die Verarbeitung beginnt mit Einrichtung, Freischaltung oder erstmaliger Nutzung des Kundenbetriebs und dauert für die Vertragslaufzeit sowie bis zum Abschluss der vereinbarten Rückgabe-, Export-, Lösch-und technisch bedingten Nachlaufprozesse.

3.2 Gegenstand, Art, Zweck, Verarbeitungsvorgänge, Kategorien betroffener Personen und Datenkategorien sind in Anlage 1 beschrieben.

3.3 BetriebPlus ist nicht für die systematische Verarbeitung von Gesundheitsdaten oder anderen besonderen Kategorien personenbezogener Daten bestimmt. Die neutrale Abwesenheitsfunktion erfasst keinen Krankheitsstatus und keinen Abwesenheitsgrund. Allgemeine Freitextfunktionen bleiben hiervon getrennt; dazu gilt Ziffer 8.

3.4 Der E-Rechnungsimport ist, soweit beim Auftraggeber freigeschaltet, Bestandteil der Auftragsverarbeitung nach Anlage 1.

4. Weisungen

4.1 BetriebPlus verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers. Weisungen ergeben sich insbesondere aus diesem AVV, dem Hauptvertrag, der zulässigen Produktkonfiguration und Nutzung durch berechtigte Nutzer sowie aus Einzelweisungen in Textform.

4.2 Weisungsberechtigt sind die vom Auftraggeber benannten Kontakte sowie nach dem Produktrollenmodell berechtigte Administratoren im Rahmen ihres Zuständigkeitsbereichs. BetriebPlus darf Identität und Berechtigung angemessen prüfen.

4.3 Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

4.4 Hält BetriebPlus eine Weisung für datenschutzrechtswidrig, informiert BetriebPlus den Auftraggeber unverzüglich. Die betroffene Verarbeitung darf bis zur Klärung ausgesetzt werden, soweit dies ohne zusätzliche Risiken möglich ist. Rechtswidrige Weisungen müssen nicht ausgeführt werden.

4.5 Soweit eine Verarbeitung aufgrund einer zwingenden gesetzlichen Verpflichtung erfolgt, informiert BetriebPlus den Auftraggeber vorab, sofern das betreffende Recht eine solche Information nicht untersagt.

4.6 Der Auftraggeber erteilt die allgemeine Weisung, bei einem konkreten Sicherheits-oder Datenschutzrisiko vorläufige Maßnahmen zu treffen, die zur Eindämmung erforderlich sind, etwa Sessionbeendigung, Zugriffsbeschränkung, Credential-Rotation, Beweissicherung oder vorübergehende Sperrung. Der Auftraggeber wird hierüber unverzüglich informiert, soweit rechtlich zulässig und sicher möglich.

5. Pflichten des Auftraggebers

5.1 Der Auftraggeber ist insbesondere verantwortlich für:

- Rechtmäßigkeit und Zweckbestimmung der Verarbeitung;
- erforderliche Rechtsgrundlagen nach Art. 6 DSGVO und gegebenenfalls nationalem Beschäftigtendatenschutzrecht;
- Transparenz-und Informationspflichten gegenüber betroffenen Personen;
- sachgerechte Rollen-, Bereichs-und Berechtigungsvergabe;
- fachliche Aufbewahrungs-und Löschfristen;
- Bearbeitung von Betroffenenrechten;
- erforderliche Mitbestimmungs-, Beteiligungs-und Dokumentationspflichten;
- die rechtmäßige Einbindung minderjähriger Beschäftigter oder Auszubildender;
- rechtmäßige Nutzung des E-Rechnungsimports und die gesetzlich erforderliche Belegaufbewahrung außerhalb eines bloßen BetriebPlus-Imports.

5.2 Der Auftraggeber weist seine Nutzer an, BetriebPlus zweckentsprechend und datensparsam zu verwenden. Insbesondere sollen keine Diagnosen, Symptome, Atteste, Arztberichte, medizinischen Unterlagen, vollständigen Personalakten, Passwörter, Secrets oder sonstigen unnötigen besonders vertraulichen Inhalte in Chat, Notizen, Aufgaben, Support oder andere allgemeine Freitextfelder eingegeben werden.

5.3 Der Auftraggeber informiert BetriebPlus, wenn sich seine Nutzung wesentlich so ändert, dass neue Datenkategorien, besondere Kategorien, neue Verarbeitungszwecke oder zusätzliche regulatorische Anforderungen entstehen können.

6. Pflichten von BetriebPlus

6.1 BetriebPlus verpflichtet sich insbesondere,

- personenbezogene Daten nur nach dokumentierter Weisung zu verarbeiten;
- die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen aufrechtzuerhalten und risikoorientiert weiterzuentwickeln;
- den Zugang zu personenbezogenen Daten auf erforderliche Personen und Systeme zu beschränken;
- zur Vertraulichkeit verpflichtete oder gesetzlich zur Verschwiegenheit verpflichtete Personen einzusetzen;
- Unterauftragsverarbeiter nur nach Ziffer 10 einzusetzen;
- den Auftraggeber bei Betroffenenrechten und den Pflichten nach Art. 32 bis 36 DSGVO nach Maßgabe dieses AVV zu unterstützen;
- Datenschutzverletzungen nach Ziffer 14 zu melden;
- nach Vertragsende Daten nach Ziffer 16 zurückzugeben, bereitzustellen, zu löschen oder zu anonymisieren;
- die zur Einhaltung von Art. 28 DSGVO erforderlichen Informationen und Nachweise bereitzustellen.

6.2 BetriebPlus verkauft Kundendaten nicht und verwendet sie nicht für personenbezogene Werbung oder zum Training eigener oder fremder KI-Modelle.

6.3 Technische Auswertungen für Sicherheit, Stabilität, Fehleranalyse und Kapazitätssteuerung werden auf das erforderliche Maß beschränkt. Personenbezogene oder kundenbeziehbare Daten werden für allgemeine Produktverbesserung nur verarbeitet, wenn hierfür eine eigene Rechtsgrundlage besteht oder eine wirksame Anonymisierung erfolgt ist.

7. Vertraulichkeit und Zugriffsberechtigung

7.1 BetriebPlus stellt sicher, dass zur Verarbeitung befugte Personen vor dem Zugriff zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.2 Zugriffe werden nach dem Need-to-know-und Least-Privilege-Prinzip vergeben. Berechtigungen werden bei Wegfall des Bedarfs entzogen oder angepasst.

7.3 Die Vertraulichkeitsverpflichtung gilt über das Ende der jeweiligen Tätigkeit und dieses AVV hinaus.

8. Besondere Kategorien und zweckwidrige sensible Inhalte

8.1 BetriebPlus fordert im vorgesehenen Produktumfang keine Gesundheitsdaten oder sonstigen besonderen Kategorien nach Art. 9 DSGVO an. Die Abwesenheitsfunktion ist neutral und enthält keinen Krankheitsstatus, Krankheitsgrund oder medizinischen Freitext.

8.2 Allgemeine Freitext-und Kommunikationsfunktionen können technisch nicht vollständig ausschließen, dass Nutzer entgegen der bestimmungsgemäßen Nutzung besondere Kategorien oder andere sensible Inhalte eingeben.

8.3 Wird BetriebPlus ein solcher Inhalt bekannt, verarbeitet BetriebPlus ihn nicht zu einem neuen eigenen Zweck. Soweit erforderlich, wird der Inhalt nach Weisung des Auftraggebers oder zur Eindämmung eines konkreten Datenschutz-oder Sicherheitsrisikos eingeschränkt, gelöscht oder anderweitig gesichert behandelt.

8.4 BetriebPlus schuldet zu diesem Zweck keine permanente inhaltliche Überwachung privater Direktkommunikation.

9. Technische und organisatorische Maßnahmen

9.1 BetriebPlus trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie des Risikos für Rechte und Freiheiten natürlicher Personen.

9.2 BetriebPlus darf Maßnahmen durch gleichwertige oder bessere Maßnahmen ersetzen, wenn das vereinbarte Schutzniveau insgesamt nicht wesentlich unterschritten wird.

9.3 Die Wirksamkeit der Maßnahmen wird regelmäßig und anlassbezogen überprüft. Art, Tiefe und Frequenz richten sich nach Risiko, Systemänderungen, Vorfällen und verfügbaren Nachweisen. Konkrete Testfrequenzen gelten nur, soweit sie gesondert dokumentiert oder vereinbart sind.

10. Unterauftragsverarbeiter

10.1 Der Auftraggeber erteilt eine allgemeine Genehmigung für die in Anlage 3 als Unterauftragsverarbeiter bezeichneten Anbieter.

10.2 BetriebPlus verpflichtet Unterauftragsverarbeiter vertraglich zu Datenschutzpflichten, die den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechen, soweit sie personenbezogene Daten des Auftraggebers verarbeiten.

10.3 BetriebPlus bleibt für die Erfüllung der gesetzlich auf BetriebPlus übertragenen Pflichten verantwortlich.

10.4 Die beabsichtigte Hinzunahme oder Ersetzung eines direkten Unterauftragsverarbeiters wird grundsätzlich mindestens 30 Kalendertage vor dem vorgesehenen Einsatz über einen dokumentierten elektronischen Kanal oder in Textform mitgeteilt. In dringenden Sicherheits-, Verfügbarkeits-oder Rechtsfällen darf die Frist angemessen verkürzt werden; die Information wird unverzüglich nachgeholt.

10.5 Der Auftraggeber kann innerhalb der Mitteilungsfrist aus nachvollziehbaren datenschutzrechtlichen Gründen widersprechen. Die Parteien suchen zunächst eine angemessene Schutzmaßnahme oder Alternative. Ist keine zumutbare Lösung möglich, kann der Auftraggeber

die konkret betroffene Leistung vor Einsatz des neuen Unterauftragsverarbeiters ohne zusätzliche Kündigungsgebühr beenden.

10.6 Anbieter, die ausschließlich Entwicklungs-, Repository-oder Monitoringinfrastruktur bereitstellen und im tatsächlichen Betriebsmodell keine personenbezogenen Kundendaten im Auftrag verarbeiten, werden nicht allein wegen ihrer technischen Nutzung als Unterauftragsverarbeiter eingeordnet.

11. Drittlandübermittlungen

11.1 Übermittlungen oder Zugriffe außerhalb des EWR erfolgen nur im Rahmen dokumentierter Weisungen und unter Einhaltung der Art. 44 ff. DSGVO.

11.2 Soweit erforderlich, werden insbesondere Angemessenheitsbeschlüsse, anwendbare Zertifizierungs-/Angemessenheitsmechanismen, Standardvertragsklauseln der Europäischen Kommission und ergänzende technische oder organisatorische Maßnahmen eingesetzt.

11.3 Die Genehmigung der in Anlage 3 beschriebenen Verarbeitungskette gilt als Weisung für die dort dokumentierten Transferkonstellationen, solange die angegebenen Schutzmechanismen bestehen.

11.4 BetriebPlus überprüft relevante Transfermechanismen anlassbezogen und bei wesentlichen Anbieter-, Rechts-oder Datenflussänderungen. Entfällt ein tragfähiger Transfermechanismus, wird eine Alternative geprüft und der Auftraggeber informiert.

12. Unterstützung bei Betroffenenrechten

12.1 BetriebPlus unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch angemessene technische und organisatorische Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und sonstigen Betroffenenrechten.

12.2 Geht eine Betroffenenanfrage unmittelbar bei BetriebPlus ein und betrifft sie Daten des Auftraggebers, wird sie ohne unangemessene Verzögerung an den Auftraggeber weitergeleitet, soweit eine Zuordnung möglich ist. Eine inhaltliche Beantwortung erfolgt nur auf Weisung oder aufgrund gesetzlicher Pflicht.

12.3 Standardunterstützung erfolgt über vorhandene Produkt-, Export-und Supportprozesse. Außergewöhnliche Zusatzleistungen können nach vorheriger Abstimmung angemessen vergütet werden, soweit dadurch die gesetzlichen Unterstützungspflichten nicht eingeschränkt werden.

13. Unterstützung nach Art. 32 bis 36 DSGVO

13.1 BetriebPlus unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der BetriebPlus verfügbaren Informationen angemessen bei:

- Sicherheit der Verarbeitung nach Art. 32 DSGVO;
- Bewertung und Dokumentation von Datenschutzverletzungen;
- Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO;
- vorherigen Konsultationen nach Art. 36 DSGVO.

13.2 BetriebPlus stellt hierfür auf Anfrage insbesondere verfügbare Beschreibungen der Verarbeitung, TOMs, Unterauftragsverarbeiterinformationen und Transferinformationen bereit, soweit keine Sicherheitsinteressen oder Rechte Dritter entgegenstehen.

13.3 Die rechtliche Entscheidung, ob eine Datenschutz-Folgenabschätzung oder vorherige Konsultation erforderlich ist, bleibt Aufgabe des Auftraggebers als Verantwortlichem.

14. Datenschutzverletzungen und Sicherheitsereignisse

14.1 BetriebPlus informiert den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, soweit Daten des Auftraggebers betroffen sind oder sein können. BetriebPlus wartet mit der Erstinformation nicht bis zum Abschluss der Untersuchung, sondern informiert so früh wie möglich, damit der Auftraggeber seine Pflichten insbesondere nach Art. 33 und 34 DSGVO fristgerecht erfüllen kann.

14.2 Die Erstmeldung enthält, soweit zum Zeitpunkt der Meldung verfügbar:

- Art und Zeitpunkt des Vorfalls;
- betroffene Systeme, Datenkategorien und Personengruppen;
- ungefähren Umfang, soweit abschätzbar;
- mögliche Folgen;
- bereits getroffene oder geplante Eindämmungsmaßnahmen;
- einen Ansprechpartner für Rückfragen.

14.3 Noch nicht verfügbare Informationen werden ohne unangemessene Verzögerung stufenweise nachgereicht.

14.4 BetriebPlus unterstützt den Auftraggeber angemessen bei Eindämmung, Risikoanalyse, Dokumentation und erforderlichen Meldungen oder Benachrichtigungen.

14.5 Nicht erfolgreiche Angriffsversuche oder technische Störungen ohne Verletzung personenbezogener Daten werden nur mitgeteilt, wenn sie für die Risikobewertung des Auftraggebers wesentlich sind.

15. Support, Logging und Fehleranalyse

15.1 Supportzugriffe auf Kundeninhalte erfolgen nur, soweit sie für eine dokumentierte Supportanfrage, Fehleranalyse, Sicherheitsmaßnahme, Vertragserfüllung oder gesetzliche Pflicht erforderlich sind.

15.2 Protokolle dienen Betrieb, Fehleranalyse, Missbrauchsabwehr, Sicherheit und Nachvollziehbarkeit. BetriebPlus gestaltet eigene Logs so, dass Passwörter, Tokens, vollständige Request-Bodies, Chattexte, Rechnungsinhalte und sensible Freitextinhalte nicht absichtlich protokolliert werden.

15.3 Provider-native Protokolle können plan-und dienstabhängige Aufbewahrungszeiten haben. Konkrete Fristen werden nur dokumentiert, wenn sie für den tatsächlich eingesetzten Dienst belegt sind.

15.4 Der Auftraggeber übermittelt im Support keine Passwörter, Atteste, medizinischen Unterlagen, vollständigen Personalakten oder ungeschwärzten vertraulichen Dokumente, soweit dies nicht im Ausnahmefall zwingend erforderlich und vorher abgestimmt ist.

16. Rückgabe, Export, Löschung und Sicherungskopien

16.1 BetriebPlus berichtigt, exportiert, löscht, anonymisiert oder schränkt personenbezogene Daten auf dokumentierte Weisung ein, soweit dies technisch möglich, rechtlich zulässig und von der Auftragsverarbeitung umfasst ist.

16.2 Anbieterwechsel und Portierung richten sich ergänzend nach Hauptvertrag und der Seite "BetriebPlus - Datenexport & Anbieterwechsel". Exportierbare Daten werden in den dort dokumentierten Formaten bereitgestellt.

16.3 Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht BetriebPlus nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück und löscht vorhandene Kopien, soweit nicht Unionsrecht oder das Recht eines Mitgliedstaats eine Speicherung verlangt. Für die Rückgabe steht nach Ende des maßgeblichen Übergangszeitraums ein Abrufzeitraum von mindestens 30 Kalendertagen zur Verfügung. Der Auftraggeber kann seine Wahl bis zum Ende dieses Abrufzeitraums in Textform erklären; wird keine Rückgabe verlangt, gilt die Löschung nach Ablauf des Abrufzeitraums als allgemeine Weisung. Gesetzliche Aufbewahrungspflichten, offene Rechtsansprüche und sonstige zwingende Gründe bleiben unberührt.

16.4 Sicherungskopien werden nach dokumentierten technischen Rotationszyklen überschrieben oder gelöscht. Eine gezielte Einzelbearbeitung historischer Sicherungen erfolgt nur, soweit technisch möglich, sicherheitsverträglich und verhältnismäßig.

16.5 Aus Sicherungskopien wiederhergestellte Daten werden wieder den geltenden Lösch-und Zugriffsvorgaben unterstellt.

16.6 BetriebPlus ersetzt kein gesetzlich erforderliches Rechnungs-oder Buchführungsarchiv des Auftraggebers. Gesetzlich aufbewahrungspflichtige Originalbelege sind vom Auftraggeber rechtzeitig in einem geeigneten System zu sichern oder zu exportieren.

17. Nachweise und Audits

17.1 BetriebPlus stellt dem Auftraggeber alle Informationen bereit, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen.

17.2 Nachweise erfolgen vorrangig durch TOM-Dokumentation, Sicherheitskonzepte, Provider-und Transferunterlagen, verfügbare Zertifikate oder Testate von Dienstleistern, Fragebögen, Remote-Auskünfte und andere geeignete Prüfmittel.

17.3 Reichen die Nachweise nach Ziffer 17.2 im Einzelfall nicht aus, ermöglicht BetriebPlus Überprüfungen einschließlich angemessener Vor-Ort-Inspektionen durch den Auftraggeber oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten und nicht mit BetriebPlus im Wettbewerb stehenden Prüfer und trägt hierzu bei. Routineprüfungen sollen mit angemessener Vorankündigung während üblicher Geschäftszeiten und grundsätzlich höchstens einmal je Kalenderjahr stattfinden. Eine zusätzliche anlassbezogene Prüfung bleibt insbesondere bei einem Datenschutzvorfall, konkreten Anhaltspunkten für eine wesentliche Pflichtverletzung oder auf Verlangen einer Aufsichtsbehörde möglich. Betriebsgeheimnisse, Sicherheit und Daten anderer Kunden sind angemessen zu schützen.

17.4 Der Auftraggeber trägt seine eigenen Auditkosten. BetriebPlus kann nur außergewöhnlichen, nachweisbaren Zusatzaufwand, der über die gesetzlich geschuldete Mitwirkung hinausgeht, nach vorheriger Abstimmung angemessen berechnen. Dies darf das gesetzliche Prüfungsrecht nicht unzumutbar erschweren. Keine Zusatzvergütung wird verlangt, soweit die Prüfung durch einen von BetriebPlus zu vertretenden Datenschutzvorfall oder eine nachgewiesene wesentliche Pflichtverletzung veranlasst ist.

17.5 Rechte von Aufsichtsbehörden bleiben unberührt.

18. Behördliche und gesetzliche Zugriffsersuchen

18.1 Erhält BetriebPlus ein verbindliches Ersuchen auf Zugriff auf Daten des Auftraggebers, informiert BetriebPlus den Auftraggeber unverzüglich, soweit dies rechtlich zulässig ist.

18.2 BetriebPlus prüft Zuständigkeit und Reichweite des Ersuchens, beschränkt Offenlegungen auf das rechtlich erforderliche Maß und nutzt verfügbare Rechtsbehelfe gegen offensichtlich rechtswidrige oder unverhältnismäßige Anforderungen, soweit dies rechtlich zulässig und zumutbar ist.

19. Verarbeitungen in eigener Verantwortlichkeit

19.1 Nicht von diesem AVV erfasst sind Verarbeitungen, für die BetriebPlus selbst Zwecke und Mittel bestimmt, insbesondere eigene Vertrags-, Abrechnungs-, Steuer-, Kontakt-, Sicherheits-, Missbrauchsabwehr-und Rechtsverteidigungsdaten.

19.2 Support-Metadaten können in eigener Verantwortlichkeit verarbeitet werden, soweit sie der Organisation und Dokumentation der Geschäftsbeziehung dienen. Ein Zugriff auf Kundeninhalte im Support erfolgt dagegen im Auftragskontext, sofern keine andere gesetzliche Rolle eingreift.

20. Haftung

20.1 Die datenschutzrechtliche Haftung der Parteien richtet sich nach Art. 82 DSGVO und sonstigem zwingenden Recht.

20.2 Ergänzend gelten die Haftungsregelungen des Hauptvertrags, soweit sie zwingenden datenschutzrechtlichen Vorschriften nicht widersprechen.

20.3 Keine Partei wird durch diesen AVV für Pflichtverletzungen verantwortlich gemacht, die ausschließlich dem Verantwortungsbereich der anderen Partei zuzurechnen sind. Zwingende gesetzliche Haftungsverteilungen bleiben unberührt.

21. Laufzeit und Beendigung

21.1 Dieser AVV gilt für die Dauer der Auftragsverarbeitung und endet erst, wenn personenbezogene Daten des Auftraggebers nach Maßgabe dieses AVV zurückgegeben, gelöscht oder wirksam anonymisiert wurden, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

21.2 Kündigung oder Beendigung des Hauptvertrags beendet nicht vorzeitig die Pflichten, die nach ihrem Zweck für Rückgabe, Löschung, Vertraulichkeit, Nachweis oder Datenschutz fortgelten müssen.

22. Schlussbestimmungen

22.1 Änderungen und Ergänzungen dieses AVV sollen in Textform dokumentiert werden. Zwingende Formvorschriften bleiben unberührt.

22.2 Sollte eine Bestimmung unwirksam sein, bleibt der übrige Vertrag wirksam; an die Stelle der unwirksamen Bestimmung tritt das dispositive Recht.

22.3 Es gilt die Rechtswahl des Hauptvertrags, soweit zwingendes Datenschutzrecht nicht entgegensteht.

Anlage 1 - Beschreibung der Verarbeitung

A. Gegenstand und Zweck

Bereitstellung und Betrieb der webbasierten Organisationssoftware BetriebPlus für interne betriebliche Organisation. Zwecke sind insbesondere Nutzer-, Rollen-und Bereichsverwaltung, Schichtplanung, Aufgaben, Urlaubs-und sonstige Anträge, neutrale Abwesenheitsmeldungen, Informationen, Meetings, einfache interne Kommunikation sowie - soweit freigeschaltet - Import, technische Verarbeitung, strukturierte Darstellung und organisatorische Verwaltung eingehender E-Rechnungen.

B. Verarbeitungsvorgänge

- Erheben, Erfassen, Speichern, Ordnen und Strukturieren;
- Anzeigen, Abfragen, Verwenden und Bereitstellen für berechtigte Nutzer;
- Übermitteln an genehmigte Unterauftragsverarbeiter;
- Berichtigen, Einschränken, Exportieren, Löschen, Pseudonymisieren und Anonymisieren;
- technisches Protokollieren, Sichern und Wiederherstellen;
- Support, Fehleranalyse, Sicherheitsüberwachung und Missbrauchsabwehr. Eine ausschließlich automatisierte Entscheidungsfindung im Sinne von Art. 22 DSGVO oder ein Beschäftigten-Scoring ist nicht Bestandteil des vorgesehenen Produktumfangs.

C. Kategorien betroffener Personen

- Beschäftigte, Mitarbeitende, Auszubildende und sonstige berechtigte Nutzer des Auftraggebers;
- Führungskräfte, Administratoren und Manager;
- eingeladene, aktive, deaktivierte oder ausgeschiedene Nutzer;
- Ansprechpartner und technische Kontakte des Auftraggebers;
- Ansprechpartner von Lieferanten und Geschäftspartnern;
- natürliche Einzelunternehmer;
- sonstige natürliche Personen, deren Angaben in eingehenden E-Rechnungen enthalten sind;
- weitere Personen nur, soweit der Auftraggeber deren Daten zulässig und bestimmungsgemäß eingibt.

D. Kategorien personenbezogener Daten

Kategorie	Beispiele
Nutzer- und Kontodaten	Name, E-Mail-Adresse, interne Nutzer-ID, Auth-ID, Rolle, Aktivstatus, Betriebs- und Bereichszuordnung
Betriebs- und Bereichsdaten	Betriebsname, geschäftliche Kontaktdaten, Branche, Bereichsname, Zuordnungen
Schichtdaten	Titel/Notiz, Beginn, Ende, Bereich, zugewiesene Person, Ersteller, Wiederholungsinformationen
Aufgabendaten	Titel, optionale Beschreibung, Status, Priorität, Fälligkeit, Bereich, Zuständige
Antragsdaten	Antragstyp, Person, Zeitraum, Bereich, optionale organisatorische Notiz, Status, Entscheidung
Abwesenheitsdaten	betroffene Person, Beginn, optional Ende oder „Ende noch unbekannt“, erforderliche Workflow-/Statusdaten; kein vorgesehener Abwesenheitsgrund
Informations- und Meetingdaten	Titel, Inhalt, Ersteller, Zielbetrieb/-bereich/-person, Zeitpunkt, Kennzeichnungen
Chat- und Kommunikationsdaten	Chatart, Mitglieder, Absender, Nachrichteninhalt, Zeitstempel, technische Lesestatus-IDs
Einladungsdaten	E-Mail-Adresse, Rolle, Bereich, Status, Token-Hash, Ablauf-/Annahme-/Widerrufszeitpunkt
Technische Daten	IP-Adresse, Browser-/Gerätedaten, Login-/Sessiondaten, Request-, Fehler-, Sicherheits- und Logmetadaten
Supportdaten im Auftragskontext	Name, E-Mail, Betrieb, Rolle, Problembeschreibung, technische Diagnoseinformationen, Supportverlauf
Lieferanten-/Geschäftspartnerdaten	Firma, Anschrift, Ansprechpartner, Kontaktdaten, soweit im Rechnungsdokument enthalten
E-Rechnungsdaten	Rechnungsnummer, Rechnungs-/Leistungsdatum, Rechnungspositionen, Beträge, Steuerinformationen, Zahlungs-/Bankinformationen, soweit enthalten

Kategorie	Beispiele
Strukturierte E-Rechnungsdaten	XML und sonstige unterstützte strukturierte Rechnungsdaten
Originaldatei/Originalrepräsentation	eingehende Originaldatei bzw. Originalrepräsentation der E-Rechnung
E-Rechnungsmetadaten	Import-, Prüf-, Status-, Zuordnungs- und technische Verarbeitungsmetadaten

E. Besondere Kategorien

Besondere Kategorien personenbezogener Daten sind kein vorgesehener Funktionsbestandteil. Die neutrale Abwesenheit erfasst keinen Krankheitsstatus und keinen medizinischen Grund. In allgemeinen Freitextfeldern können Nutzer entgegen der bestimmungsgemäßen Nutzung gleichwohl besondere Kategorien eingeben; dafür gelten Ziffer 8 des AVV und die Nutzungsregeln des Hauptvertrags.

F. Fachliche Speicher-und Löschlogik

1. Der Auftraggeber bestimmt fachliche Aufbewahrungsfristen und Löschweisungen, soweit das Produkt hierfür konfigurierbare oder operative Prozesse bereitstellt.
2. Nach Vertragsende gelten die Export-, Wechsel-, Abruf-und Löschprozesse des Hauptvertrags.
3. Schichtdaten sind organisatorische Planungs-und Historiendaten, nicht automatisch gesetzlicher Arbeitszeitnachweis.
4. E-Rechnungsdaten werden nach Weisung und Vertragszweck gespeichert. Gesetzliche Aufbewahrungspflichten des Auftraggebers bestehen unabhängig hiervon; BetriebPlus ist kein revisionssicheres Archiv.
5. Routine-und Sicherheitslogs werden nur solange aufbewahrt, wie dies für Betrieb, Fehleranalyse, Sicherheit, Nachweis oder gesetzliche Pflichten erforderlich ist. Konkrete providerseitige Fristen richten sich nach dem tatsächlich eingesetzten Tarif und Dienst.
6. Sicherungskopien werden nach dokumentierten technischen Rotationszyklen überschrieben oder gelöscht.

G. Verarbeitungsorte

Die primäre Produktkonfiguration ist auf eine EU-Primärregion für Datenbank-und produktiv relevante dynamische Verarbeitung ausgerichtet. Ergänzende Drittlandbezüge können sich aus Anbieterorganisation, Support, CDN, Unterauftragsverarbeitern und Plattformbetrieb ergeben; sie richten sich nach Anlage 3 und den Art. 44 ff. DSGVO.

Anlage 2 - Technische und organisatorische Maßnahmen (TOMs)

Die nachfolgenden Maßnahmen beschreiben das für den BetriebPlus-Pilot und den anschließenden SaaS-Betrieb vorgesehene Schutzniveau. Konkrete Providerparameter, Rotationsfristen, RTO/RPO-Werte oder Zertifizierungen gelten nur, soweit sie ausdrücklich gesondert dokumentiert sind.

1. Vertraulichkeit

- Vertraulichkeitsverpflichtung für zugriffsberechtigte Personen;
- Need-to-know-und Least-Privilege-Prinzip;
- Trennung von Entwicklungs-, Administrations-und produktiven Aufgaben, soweit organisatorisch erforderlich;
- Verbot produktiver Kundendaten in Quellcode-Repositories und nicht freigegebenen Entwicklungsumgebungen.

2. Authentifizierung

- persönliche Nutzerkonten;
- zentrale Authentifizierungs-und Sessionverwaltung;
- sichere Passwortverarbeitung über den eingesetzten Authentifizierungsdienst;
- Betreiberzugänge werden nach Schutzbedarf zusätzlich abgesichert;
- Deaktivierung oder Entzug von Zugängen bei Wegfall der Berechtigung.

3. Rollen-und Berechtigungsmodell

- Rollen Admin, Manager und Mitarbeiter;
- bereichs-/departmentbezogene Sicht-und Bearbeitungsrechte;
- objekt-und mitgliedschaftsbezogene Regeln, wo die Funktion dies erfordert;
- private Direktchats werden über Mitgliedschaft und nicht allein über eine Managementrolle autorisiert.

4. Serverseitige Autorisierung

- produktiv relevante Fachzugriffe werden serverseitig geprüft;
- Clientwerte wie Company-ID, Rollenangabe oder Nutzer-ID sind nicht alleinige Berechtigungsgrundlage;
- Company-, Rollen-, Department-, Objekt-und Mitgliedschaftsprüfungen werden für die relevanten Datenpfade durchgesetzt.

5. Mandanten-und Trennungskontrolle

- logische Mandantentrennung anhand des Kundenbetriebs;
- serverseitige Prüfung der Mandantenzugehörigkeit;
- Datenbankberechtigungen auf erforderliche Zugriffe beschränkt;
- RLS/datenbankseitige Policies bilden eine zusätzliche Schutzschicht für produktiv relevante Datenpfade.

6. Least Privilege und produktive Berechtigungen

- produktive Runtime-und Datenbankberechtigungen werden auf das erforderliche Maß begrenzt;
- privilegierte Service-oder Secret-Credentials werden nicht als normaler Clientzugang verwendet;
- privilegierte Zugriffe werden nur für Betrieb, Support, Migration, Sicherheit oder Wiederherstellung eingesetzt.

7. Transport-und Speicherschutz

- verschlüsselte Transportverbindungen für produktive Webzugriffe;
- Nutzung der vom Provider bereitgestellten Speicherschutzmechanismen;
- private Speicherung von E-Rechnungsoriginalen im vorgesehenen Storage-Pfad;
- keine dauerhaften öffentlichen Links für vertrauliche Originaldateien als vorgesehener Produktpfad.

8. Secret-und Credential-Management

- Secrets ausschließlich in vorgesehenen Secret-Speichern und Konfigurationswegen;
- keine Secrets in Quellcode, Chat, Supportticket oder allgemeiner Dokumentation;
- Rotation bei Verdacht auf Kompromittierung;
- Zugriff auf Secrets nur für erforderliche Betreiberfunktionen.

9. Protokollierung und Nachvollziehbarkeit

- technische Logs für Betrieb, Fehleranalyse, Sicherheit und Missbrauchsabwehr;
- keine absichtliche Protokollierung von Passwörtern, Tokens, vollständigen Request-Bodies, Chatinhalten oder Rechnungsinhalten;
- Reduktion oder Maskierung personenbezogener Identifikatoren, soweit mit dem Sicherheitszweck vereinbar;
- separate Vorfall-und Sicherheitsdokumentation für relevante Ereignisse.

10. Integrität und Änderungskontrolle

- kontrollierte Deployment-und Änderungsprozesse;
- Code-und Konfigurationsänderungen über versionierte Entwicklungsabläufe;
- Prüfung sicherheitsrelevanter Änderungen vor produktiver Freigabe;
- kontrollierte Datenbank-und Berechtigungsänderungen.

11. Backup und Wiederherstellung

- Sicherung produktiv relevanter Daten nach dokumentiertem Backup-Konzept;
- Trennung von Primärdaten, Datenbank-Backups und Object Storage;
- Wiederherstellungsverfahren für relevante Datenpfade;
- Sicherungskopien werden nicht als regulärer Produktivspeicher verwendet;
- Restore-Vorgänge unterliegen Zugriffskontrolle und nachgelagerter Löschlogik.

12. Verfügbarkeit und Resilienz

- Nutzung professioneller Hosting-, Datenbank-und Infrastrukturprovider;
- Monitoring ausgewählter öffentlicher oder datenminimierter Endpunkte;
- Notfallmaßnahmen für Störungen und Sicherheitsereignisse;
- Deployment-/Rollback-Möglichkeiten, soweit technisch für den betroffenen Pfad vorhanden;
- keine vertragliche RTO-/RPO-oder Verfügbarkeitszahl in diesen TOMs, soweit nicht gesondert vereinbart.

13. Löschung und Retention

- Löschung/Anonymisierung aktiver Primärdaten nach Weisung und Vertragsende;
- dokumentierte technische Nachlauf-und Backupzyklen;
- getrennte Behandlung von Live-Daten, Logs, Mail-/Supportdaten, Backups und Object Storage;
- fachliche Fristen des Auftraggebers bleiben maßgeblich.

14. Incident Management

- definierter Melde-und Eskalationsprozess;
- Eindämmung, Beweissicherung, Ursachenanalyse und Wiederherstellung;
- Datenschutzverletzungen werden dem Auftraggeber ohne unangemessene Verzögerung gemeldet;
- gestufte Nachmeldung unvollständiger Informationen.

15. Change-, Deployment-und Testprozesse

- Änderungen werden vor produktiver Nutzung angemessen geprüft;
- besonders sicherheitsrelevante Datenpfade unterliegen zusätzlichen Freigabeprüfungen;
- Testdaten werden nach Möglichkeit synthetisch oder anonymisiert verwendet;
- produktive Echtdaten werden nicht in nicht freigegebene Test-oder KI-Umgebungen kopiert.

16. Auftragskontrolle

- Einsatz von Unterauftragsverarbeitern nach AVV;
- Prüfung verfügbarer DPA-/SCC-/Subprozessorinformationen;
- Änderungskommunikation und Widerspruchsprozess;
- Providerzugriffe werden nach Vertrags-und Sicherheitslage bewertet.

17. Weitergabe-und Transferkontrolle

- dokumentierte Datenflüsse und Verarbeitungsorte;
- Nutzung geeigneter Transferinstrumente bei Drittlandbezug;
- Datenminimierung für CDN, Monitoring, Logs und Support;
- keine sensiblen Daten in Monitor-URLs oder öffentlich erreichbaren Health-Endpunkten.

18. Regelmäßige Wirksamkeitsprüfung

- risikobasierte Überprüfung der TOMs;
- anlassbezogene Prüfung bei wesentlichen Architektur-, Provider-, Rollen-oder Rechtsänderungen;
- Nachverfolgung festgestellter Abweichungen;
- keine Behauptung einer BetriebPlus-eigenen ISO-, SOC-oder BSI-Zertifizierung, sofern eine solche nicht besteht.

Anlage 3 - Unterauftragsverarbeiter und technische Dienstleister

A. Genehmigte direkte Unterauftragsverarbeiter

Dienstleister	Zweck	Primärer Daten-/Standortbezug	Vertragliche Absicherung
Vercel Inc., USA	Hosting, CDN, Deployment, serverseitige Web-/API-Funktionen, technische Runtime-/Build-Protokolle	dynamische Verarbeitung ist nach der dokumentierten Konfiguration auf eine EU-Region ausgerichtet; Anbieter- und Subprozessorbezug kann Drittländer einschließen	Vercel-Datenschutzbedingungen/ DPA einschließlich anwendbarer Transfermechanismen und Subprozessorregelungen; konkrete Plan-/Vertragslage ist vor Freigabe zu verifizieren
SUPABASE PTE. LTD., Singapur	PostgreSQL, Authentifizierung, Sessions, Plattform-/ Datenbankprotokolle, Backups, privater Object Storage für freigeschaltete Funktionen	primäre BetriebPlus-Projektregion ist nach der dokumentierten Konfiguration Frankfurt/EU; mögliche Support- und Subprozessorzugriffe außerhalb des EWR	Supabase-Datenschutzregelung/ DPA einschließlich einschlägiger Transfermechanismen und Subprozessorregelungen; Vertragspartner/Projektregion sind vor Freigabe zu verifizieren
IONOS SE, Deutschland	geschäftliche E-Mail-Postfächer, SMTP-Versand, Einladungs-/ Resetmails und Supportkommunikation	Deutschland/EU; weitere Anbieterketten nach IONOS-Unterlagen	AVV/AV-Regelung nach dokumentierter Vertragslage; tatsächlicher Abschluss ist vor Freigabe zu verifizieren

B. Technischer Dienstleister ohne planmäßigen Zugriff auf Kundeninhalte

Dienstleister	Zweck	Einordnung
UptimeRobot s. r. o., Slowakei	Verfügbarkeitsmonitoring öffentlicher bzw. datenminimierter Endpunkte und Alarmierung	kein planmäßiger Abruf geschützter App-Inhalte oder Kundeninhalte; soweit im Einzelfall personenbezogene Daten im Auftrag verarbeitet werden, gelten DPA und Art.-28-Anforderungen

C. Entwicklungs-/Repository-Infrastruktur

GitHub wird für Quellcode und Entwicklungsworkflow eingesetzt. Produktive Kunden-, Beschäftigten-oder Rechnungsdaten, Datenbank-Dumps und Secrets sind dort kein zulässiger Inhalt. GitHub wird deshalb im vorgesehenen Betriebsmodell nicht allein wegen der Repository-Nutzung als Unterauftragsverarbeiter für Kundendaten aufgeführt.

D. Drittlandtransfers

Drittlandbezüge können insbesondere aus US-Anbieterorganisationen, Support, CDN, Plattformbetrieb und Unterauftragsverarbeitern entstehen. BetriebPlus dokumentiert die einschlägigen Transferinstrumente intern und hält die Verarbeitungskette aktuell.

Anlage 4 - Standardweisungen und Kontakte

1. Standardweisungen ergeben sich aus Hauptvertrag, diesem AVV, der Produktkonfiguration und der berechtigten Nutzung.
2. Einzelweisungen sind an datenschutz@betriebplus.com oder einen vereinbarten sicheren Kanal zu richten.
3. Sicherheitsmeldungen sind zusätzlich an support@betriebplus.com möglich.
4. Der Auftraggeber benennt mindestens einen Vertrags-/Datenschutzkontakt und hält dessen Kontaktdaten aktuell.
5. Lösch-, Export-oder Schließungsweisungen mit erheblicher Wirkung dürfen von BetriebPlus vor Ausführung angemessen authentifiziert werden.