

Vereinbarung zur Auftragsverarbeitung

gemäß Artikel 28 Datenschutz-Grundverordnung (DSGVO)

Vertragsfassung	Auftragsverarbeiter
Version 1.1 (Entwurf) Stand: 24. August 2026	Betty & June Digital UG (haftungsbeschränkt) Kiefernring 9, 15806 Zossen Deutschland

Elektronischer Abschluss. Diese Vereinbarung wird bei der Registrierung eines kostenpflichtigen B2B-Kontos durch ausdrückliche Zustimmung abgeschlossen. Die Identität des Verantwortlichen ergibt sich aus den Registrierungs-, Studio- und Abrechnungsdaten sowie dem gespeicherten Zustimmungsnachweis.

Auftragsverarbeiter:

Betty & June Digital UG (haftungsbeschränkt), Kiefernring 9, 15806 Zossen, vertreten durch Geschäftsführer Rodney Bleßmann, Amtsgericht Potsdam, HRB 42559, E-Mail: hello@bettyjunedigital.com

Verantwortlicher:

Die natürliche oder juristische Person, die bei der Registrierung eines kostenpflichtigen Kontos für missbettyjune.com als Unternehmen oder selbstständig tätige Person identifiziert wird und durch eine vertretungsberechtigte Person dieser Vereinbarung zustimmt (nachfolgend „Kunde“).

Präambel

Betty & June Digital UG (haftungsbeschränkt) stellt das SaaS-Produkt missbettyjune.com bereit. Der Kunde nutzt missbettyjune.com zur Organisation seiner geschäftlichen Studioabläufe. Soweit Betty & June Digital dabei personenbezogene Daten nach Weisung des Kunden verarbeitet, handelt Betty & June Digital als Auftragsverarbeiter. Der Kunde bleibt Verantwortlicher für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Rechte betroffener Personen.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien. Sie ergänzt den Vertrag über die Nutzung von missbettyjune.com (Hauptvertrag). Bei Widersprüchen gehen die Regelungen dieser Vereinbarung für die Auftragsverarbeitung vor.

§ 1 Begriffe und Anwendungsbereich

- (1) Es gelten die Begriffsbestimmungen der DSGVO, insbesondere „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Unterauftragsverarbeiter“ und „Datenschutzverletzung“.
- (2) Diese Vereinbarung gilt für alle personenbezogenen Daten, die Betty & June Digital bei Bereitstellung, Betrieb, Wartung oder Support von missbettyjune.com im Auftrag des Kunden verarbeitet. Die Einzelheiten ergeben sich aus Anlage 1.
- (3) Die Vereinbarung erfasst alle Studios desselben rechtlichen Kundenunternehmens, die unter dessen Konto bei missbettyjune.com betrieben werden. Werden über ein Konto Studios unterschiedlicher rechtlicher Betreiber verwaltet, muss jeder Betreiber vor Beginn seiner Verarbeitung einen eigenen AVV abschließen.
- (4) Persönliche Konten von eingeladenen Teammitgliedern, einschließlich Free-Konten, werden nicht selbst Partei dieses AVV. Ihre Verarbeitung von Studio-, Kunden- oder Termindaten erfolgt als autorisierte Nutzung unter Verantwortung des jeweiligen Kunden.
- (5) Verarbeitungen, bei denen Betty & June Digital eigene Zwecke und Mittel bestimmt, fallen nicht unter diesen AVV. Dazu zählen insbesondere Vertrags- und Abrechnungsverwaltung gegenüber dem direkten Kunden von missbettyjune.com, Erfüllung eigener gesetzlicher Pflichten sowie notwendige Verarbeitung zur allgemeinen Missbrauchs- und Systemsicherheit. Hierüber informiert die Datenschutzerklärung von Betty & June Digital.

§ 2 Gegenstand, Art, Zweck und Dauer

- (1) Gegenstand ist die technische Bereitstellung der mandantenfähigen SaaS-Anwendung missbettyjune.com durch Betty & June Digital einschließlich Hosting, Datenbankbetrieb, Dateiablage, Benutzer- und Rechteverwaltung, Sicherung, Wartung, Fehleranalyse und Support.
- (2) Die Verarbeitung umfasst je nach Nutzung insbesondere Erheben, Erfassen, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Anzeigen, Übermitteln, Einschränken, Anonymisieren, Sichern und Löschen personenbezogener Daten.
- (3) Zwecke sind insbesondere Kunden- und Terminverwaltung, Personal- und Einsatzplanung, Aufgabenverwaltung, Verwaltung von Leistungen, Produkten und Ressourcen, Rechnungs- und Belegverwaltung, Gutschein- und Aktionsverwaltung, öffentliche Studio- und Teamprofile sowie sichere Kontoführung.

(4) Die Auftragsverarbeitung beginnt mit der elektronischen Zustimmung und dauert, solange Betty & June Digital über missbettyjune.com Daten des Kunden verarbeitet. Ein Wechsel in den Free-Plan beendet den AVV nicht, wenn Daten weiterhin gespeichert werden. Die Vereinbarung endet erst nach Abschluss der geregelten Rückgabe oder Löschung einschließlich der Backup-Rotation. Für persönliche Free-Teamkonten, die kein eigener Kunde im Sinne dieser Vereinbarung sind, gilt § 15 Absatz 3.

§ 3 Verantwortlichkeit und Pflichten des Kunden

(1) Der Kunde entscheidet über Zwecke und wesentliche Mittel seiner fachlichen Verarbeitungen und stellt deren Rechtmäßigkeit sicher. Er ist insbesondere verantwortlich für Rechtsgrundlagen, Informationspflichten, Einwilligungen, Datenminimierung, Richtigkeit, Aufbewahrungsfristen und die Bearbeitung von Betroffenenrechten.

(2) Der Kunde darf besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, nur eingeben, wenn dies erforderlich ist und eine Ausnahme nach Art. 9 Abs. 2 DSGVO sowie eine Rechtsgrundlage nach Art. 6 DSGVO vorliegt. Freitextfelder sind auf das notwendige Maß zu beschränken.

(3) Bei Daten Minderjähriger stellt der Kunde die besondere Schutzbedürftigkeit, die Rechtmäßigkeit der Verarbeitung und gegebenenfalls erforderliche Zustimmungen der Sorgeberechtigten sicher.

(4) Der Kunde vergibt Zugriffsrechte nach dem Erforderlichkeitsprinzip, lädt nur berechtigte Personen ein, überprüft Berechtigungen regelmäßig und entzieht sie unverzüglich, wenn sie nicht mehr benötigt werden.

(5) Der Kunde übermittelt keine rechtswidrigen Inhalte und keine Daten, deren Verarbeitung mit dem vereinbarten Leistungsumfang unvereinbar ist. Er informiert Betty & June Digital unverzüglich über erkennbare Fehler, unbefugte Zugriffe oder rechtswidrige Weisungen.

§ 4 Weisungen

(1) Betty & June Digital verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, soweit keine gesetzliche Verpflichtung zur Verarbeitung besteht. Die bestimmungsgemäße Nutzung der Funktionen von missbettyjune.com gilt als dokumentierte Weisung.

(2) Einzelweisungen können durch vertretungsberechtigte oder im Kundenkonto autorisierte Personen in Textform an hello@bettyjunedigital.com erteilt werden. Weisungen außerhalb des vereinbarten Leistungsumfangs können nach vorheriger Abstimmung gesondert vergütet werden.

(3) Hält Betty & June Digital eine Weisung für datenschutzwidrig, wird der Kunde unverzüglich informiert. Die Ausführung darf bis zur Bestätigung oder Änderung der Weisung ausgesetzt werden, soweit dies zum Schutz der Daten erforderlich ist.

(4) Ist Betty & June Digital gesetzlich zu einer nicht angewiesenen Verarbeitung verpflichtet, wird der Kunde vorab informiert, soweit das Gesetz dies nicht aus wichtigem öffentlichen Interesse untersagt.

§ 5 Vertraulichkeit und zugriffsberechtigte Personen

(1) Betty & June Digital stellt sicher, dass alle zur Verarbeitung befugten Personen vor dem Zugriff auf Vertraulichkeit verpflichtet oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterworfen sind und nur nach dokumentierter Weisung handeln.

(2) Zugriffe auf Produktivdaten erfolgen nur, soweit sie für Betrieb, Wartung, Sicherheit, Fehleranalyse oder angewiesenen Support erforderlich sind. Eine routinemäßige inhaltliche Einsichtnahme findet nicht statt.

(3) Zugriffsrechte werden individuell vergeben, regelmäßig überprüft und nach Wegfall des Bedarfs unverzüglich entzogen. Gemeinsam genutzte Administratorzugänge sind zu vermeiden.

(4) Eingeladene Benutzer des Kunden handeln unter dessen Verantwortung. Betty & June Digital stellt technische Rollen und Berechtigungen bereit; der Kunde bleibt für ihre konkrete Vergabe verantwortlich.

§ 6 Technische und organisatorische Maßnahmen

(1) Betty & June Digital trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen, Zwecken und Risiken geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

(2) Die vereinbarten Maßnahmen sind in Anlage 3 beschrieben. Sie umfassen insbesondere Zugangs- und Zugriffskontrolle, Verschlüsselung bei der Übertragung, Mandantentrennung, Verfügbarkeits- und Wiederherstellungsmaßnahmen, Protokollierung, sichere Entwicklung und Verfahren zur regelmäßigen Überprüfung.

(3) Betty & June Digital darf Maßnahmen an die technische Entwicklung anpassen, sofern das vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Verschlechterungen sind unzulässig.

§ 7 Unterstützung bei Betroffenenrechten

(1) Betty & June Digital unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und beim Umgang mit automatisierten Entscheidungen, soweit einschlägig.

(2) Direkt an Betty & June Digital gerichtete Anfragen zu Kundendaten werden unverzüglich an den zuständigen Kunden weitergeleitet. Eine inhaltliche Antwort an die betroffene Person erfolgt nur auf Weisung des Kunden, soweit keine eigene gesetzliche Pflicht besteht.

(3) Eine erste Reaktion auf ordnungsgemäß zugeordnete Unterstützungsanfragen erfolgt normalerweise innerhalb von fünf Arbeitstagen. Drohende gesetzliche Fristabläufe oder hohe Risiken werden priorisiert.

(4) Übliche Unterstützung ist mit der Vergütung des Hauptvertrags abgegolten. Außergewöhnlicher, nicht durch eine Pflichtverletzung von Betty & June Digital verursachter Aufwand kann nach vorheriger Abstimmung gesondert berechnet werden.

(5) Wird im Rahmen von Absatz 1 während der laufenden Vertragsnutzung eine Löschung einzelner Daten vorgenommen, gilt für deren Entfernung aus turnusmäßigen Sicherungskopien die in § 10 Absatz 3 beschriebene Backup-Rotation entsprechend. Eine sofortige, isolierte Löschung aus einzelnen Sicherungssätzen ist auch in diesem Fall technisch nicht vorgesehen.

§ 8 Datenschutzverletzungen

(1) Betty & June Digital informiert den Kunden unverzüglich, nachdem eine Verletzung des Schutzes der im Auftrag verarbeiteten personenbezogenen Daten bekannt geworden ist. Angestrebt wird eine Erstmeldung

innerhalb von 24 Stunden nach Bekanntwerden.

(2) Die Meldung enthält, soweit zu diesem Zeitpunkt verfügbar, Art des Vorfalls, Kategorien und ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie eine Kontaktmöglichkeit. Fehlende Informationen werden schrittweise nachgereicht.

(3) Betty & June Digital dokumentiert relevante Tatsachen, Auswirkungen und Abhilfemaßnahmen und unterstützt den Kunden bei Meldungen nach Art. 33 DSGVO und Benachrichtigungen nach Art. 34 DSGVO.

(4) Die Information stellt kein Anerkenntnis einer Rechtspflicht oder Verantwortlichkeit dar. Der Kunde entscheidet über seine Meldung an Aufsichtsbehörden und betroffene Personen.

§ 9 Datenschutz-Folgenabschätzung und Behörden

(1) Betty & June Digital unterstützt den Kunden unter Berücksichtigung der verfügbaren Informationen bei Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO und gegebenenfalls vorherigen Konsultationen nach Art. 36 DSGVO. Anfragen von Aufsichtsbehörden zu Kundendaten werden, soweit zulässig, unverzüglich an den Kunden weitergeleitet.

(2) Üblicher Unterstützungsaufwand ist mit der Vergütung des Hauptvertrags abgegolten. Für außergewöhnlichen, nicht durch eine Pflichtverletzung von Betty & June Digital verursachten Aufwand gilt § 7 Absatz 4 entsprechend.

§ 10 Rückgabe, Löschung und Vertragsende

(1) Nach vollständiger Beendigung der Nutzung erhält der Kunde für 30 Tage Gelegenheit, die Rückgabe oder Bereitstellung seiner Daten in einem geeigneten, gängigen Format anzufordern. Bis ein vollständiger Selbstbedienungsexport verfügbar ist, erfolgt die Bereitstellung auf Anfrage.

(2) Nach Ablauf des Übergangszeitraums werden die produktiven Kundendaten innerhalb von 30 Tagen gelöscht oder, wo vereinbart und sachgerecht, anonymisiert. Gesetzlich aufzubewahrende Daten werden gesperrt und ausschließlich für den gesetzlichen Zweck verwendet.

(3) Gelöschte Daten entfallen im Rahmen einer 30-tägigen Backup-Rotation spätestens innerhalb weiterer 30 Tage aus den Sicherungen. Eine selektive Löschung aus einzelnen Sicherungssätzen ist technisch nicht vorgesehen. Bei einem zwingenden Gesamtsystem-Restore gelten die Löschkennzeichen und -prozesse erneut. Für Löschungen während der laufenden Vertragsnutzung gilt § 7 Absatz 5.

(4) Die Löschung eines einzelnen Benutzerkontos löscht gemeinsam genutzte Studiodaten nicht, wenn andere berechnete Benutzer das Studio weiterführen. Die Verantwortung wird einem verbleibenden berechtigten Inhaber zugeordnet.

(5) Auf Anfrage bestätigt Betty & June Digital die vertragsgemäße Löschung, soweit keine gesetzliche Aufbewahrung entgegensteht.

§ 11 Unterauftragsverarbeiter

(1) Der Kunde erteilt die allgemeine schriftliche Genehmigung zur Beauftragung der in Anlage 2 genannten Unterauftragsverarbeiter.

(2) Betty & June Digital informiert den Kunden mindestens 14 Tage vor der beabsichtigten Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform, insbesondere per E-Mail oder Mitteilung im Kundenkonto. Die Information bezeichnet Anbieter, Ort und Aufgabe.

(3) Der Kunde kann innerhalb der Frist aus nachvollziehbaren Datenschutzgründen widersprechen. Die Parteien suchen zunächst eine zumutbare Lösung. Ist eine Lösung nicht möglich, kann der betroffene Dienst oder Vertragsteil beendet werden.

(4) Bei einer aus dringenden Sicherheits- oder Verfügbarkeitsgründen notwendigen Änderung kann die Vorabfrist ausnahmsweise verkürzt werden. Betty & June Digital informiert den Kunden unverzüglich und begründet die Dringlichkeit.

(5) Unterauftragsverarbeitern werden durch Vertrag im Wesentlichen dieselben Datenschutzpflichten auferlegt. Betty & June Digital bleibt gegenüber dem Kunden für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

(6) Auf Verlangen stellt Betty & June Digital eine Kopie der relevanten Datenschutzregelungen mit Unterauftragsverarbeitern bereit; Geschäftsgeheimnisse und nicht erforderliche Informationen dürfen geschwärzt werden.

§ 12 Datenübermittlungen in Drittländer

(1) Übermittlungen an ein Drittland oder eine internationale Organisation erfolgen nur auf dokumentierte Weisung oder auf Grundlage einer gesetzlichen Verpflichtung und unter Einhaltung von Kapitel V DSGVO.

(2) Der Kernbetrieb von Server, Datenbank und Dateiablage erfolgt in Deutschland. Beim E-Mail-Versand über Microsoft 365 können nach den Microsoft-Vertragsunterlagen und der jeweils aktuellen Unterauftragnehmer- und Personalstandortdokumentation internationale Zugriffe oder weitere Übermittlungen nicht vollständig ausgeschlossen werden.

(3) Soweit kein Angemessenheitsbeschluss greift, stellt Betty & June Digital sicher, dass geeignete Garantien bestehen, insbesondere anwendbare EU-Standardvertragsklauseln und ergänzende technische oder organisatorische Maßnahmen.

(4) Die Wirksamkeit einzelner internationaler Angemessenheitsbeschlüsse, insbesondere des EU-US Data Privacy Framework, wird derzeit rechtlich und politisch diskutiert und kann sich ändern. Unabhängig vom Fortbestand eines solchen Beschlusses stellt Betty & June Digital sicher, dass die in Absatz 3 genannten Garantien als Auffanglösung wirksam bleiben, und beobachtet die Rechtsentwicklung.

§ 13 Nachweise und Kontrollen

(1) Betty & June Digital stellt dem Kunden alle Informationen zur Verfügung, die zum Nachweis der Pflichten aus Art. 28 DSGVO erforderlich sind, und ermöglicht angemessene Überprüfungen.

(2) Kontrollen erfolgen vorrangig durch Dokumentenprüfung, Fragebogen oder Fernprüfung. Vor-Ort-Prüfungen sind bei berechtigtem Anlass und grundsätzlich mit mindestens 14 Tagen Vorankündigung während üblicher Geschäftszeiten möglich.

(3) Prüfer müssen fachkundig, unabhängig und zur Vertraulichkeit verpflichtet sein. Direkte Wettbewerber von Betty & June Digital können abgelehnt werden, soweit ein gleichwertiger unabhängiger Prüfer zur Verfügung

steht.

(4) Prüfungen dürfen den Betrieb, die Sicherheit, Geschäftsgeheimnisse oder Rechte anderer Kunden nicht unverhältnismäßig beeinträchtigen. Ein direkter Zugriff auf Daten anderer Mandanten ist ausgeschlossen.

(5) Regelprüfungen finden höchstens einmal jährlich statt. Zusätzliche Prüfungen bleiben bei konkretem Verdacht, Datenschutzverletzungen oder behördlicher Anordnung zulässig. Außergewöhnliche Kosten trägt der Kunde, sofern kein erheblicher Verstoß von Betty & June Digital festgestellt wird.

§ 14 Haftung

(1) Für die Haftung gelten Art. 82 DSGVO und die Regelungen des Hauptvertrags. Keine Bestimmung dieses AVV beschränkt gesetzliche Rechte betroffener Personen oder Befugnisse von Aufsichtsbehörden.

(2) Werden Betty & June Digital und der Kunde gegenüber einer betroffenen Person nach Art. 82 DSGVO gesamtschuldnerisch in Anspruch genommen, richtet sich der interne Ausgleich zwischen den Parteien nach dem jeweiligen Verantwortungsanteil an der Pflichtverletzung. Soweit der Kunde für den zugrundeliegenden Verstoß verantwortlich ist, insbesondere durch rechtswidrige Weisungen, unzulässige Inhalte oder eine Verletzung seiner Pflichten aus § 3, stellt er Betty & June Digital in entsprechendem Umfang von Ansprüchen Dritter, angemessenen Rechtsverteidigungskosten und eigenen Schäden frei.

(3) Im Übrigen gelten die Haftungsbeschränkungen und -ausschlüsse des Hauptvertrags, soweit gesetzlich zulässig, auch für Ansprüche im Zusammenhang mit dieser Vereinbarung. Ansprüche betroffener Personen nach Art. 82 DSGVO bleiben hiervon unberührt.

§ 15 Elektronischer Abschluss und Versionsnachweis

(1) Diese Vereinbarung wird elektronisch abgeschlossen. Die registrierende Person bestätigt über eine nicht vorausgewählte Pflicht-Checkbox, für den im Konto angegebenen B2B-Kunden vertretungsberechtigt zu sein und der bezeichneten Vertragsversion zuzustimmen. Bei begründeten Zweifeln an der Vertretungsberechtigung kann Betty & June Digital einen zusätzlichen Nachweis verlangen und die Freischaltung der Verarbeitung bis dahin zurückstellen.

(2) Betty & June Digital speichert mindestens Kunden- und Benutzer-ID, Name, E-Mail-Adresse, Zeitpunkt, AVV-Version und eine technische Prüfsumme der bereitgestellten Vertragsdatei. Die akzeptierte Fassung bleibt abrufbar.

(3) Free-Teamkonten schließen keinen eigenen AVV ab. Wird ein solches Konto später selbst Betreiber eines kostenpflichtigen Studios, ist der AVV vor Aktivierung der entsprechenden Verarbeitung zu akzeptieren.

(4) Wesentliche Änderungen des AVV erfordern eine erneute Zustimmung. Änderungen der Unterauftragnehmer richten sich ausschließlich nach § 11.

§ 16 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform, soweit nicht die vereinbarte elektronische Zustimmungsform oder eine strengere gesetzliche Form gilt.

(2) Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die Bestimmung durch eine wirksame Regelung, die ihrem datenschutzrechtlichen Zweck am nächsten kommt.

(3) Es gilt deutsches Recht. Zwingende Datenschutzvorschriften und Zuständigkeiten der Aufsichtsbehörden bleiben unberührt.

(4) Anlagen 1 bis 4 sind Bestandteil dieser Vereinbarung.

Anlage 1 – Beschreibung der Auftragsverarbeitung

1. Gegenstand und Zwecke

- Bereitstellung und Betrieb der mandantenfähigen SaaS-Anwendung missbettyjune.com durch Betty & June Digital.
- Verwaltung von Studios, Teams, Mitarbeitern, Kunden, Terminen, Aufgaben, Arbeitszeiten und Abwesenheiten.
- Verwaltung von Leistungen, Produkten, Ressourcen, Rechnungen, Zahlungen, Gutscheinen und Aktionen.
- Bereitstellung öffentlicher Studio- und Teamprofile nach den Einstellungen des Kunden.
- Authentifizierung, Rechteverwaltung, Sicherheitsprotokollierung, Support, Datensicherung und Wiederherstellung.

2. Art der Verarbeitung

Erheben, Erfassen, Strukturieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Anzeigen, Offenlegen durch angewiesene Übermittlung, Abgleichen, Verknüpfen, Einschränken, Sichern, Wiederherstellen, Anonymisieren und Löschen. Die Verarbeitung erfolgt fortlaufend nach Nutzung durch den Kunden.

3. Kategorien betroffener Personen

- Inhaber, vertretungsberechtigte Personen und Ansprechpartner des Kunden.
- Beschäftigte, freie Mitarbeiter, Bewerber, Teammitglieder und eingeladene Benutzer des Studios.
- Kundinnen und Kunden, Interessenten, Terminpersonen, Rechnungsempfänger, Gutscheinempfänger und Kontaktpersonen.
- Minderjährige Kundinnen und Kunden, soweit der Kunde deren Daten rechtmäßig in missbettyjune.com verarbeitet.
- Besucher öffentlicher Studioseiten und Benutzer der Terminverfügbarkeitsfunktionen, soweit personenbezogene Daten anfallen.

4. Kategorien personenbezogener Daten

Kategorie	Beispiele
Identitäts- und Stammdaten	Name, Vorname, Benutzer-ID, Kundennummer, Geburtstag, Rollen- und Studiozuordnung
Kontakt- und Adressdaten	E-Mail-Adresse, Telefonnummer, Postanschrift, öffentliche Kontaktangaben
Beschäftigten- und Organisationsdaten	Funktion, Rolle, Berechtigungen, Arbeitszeiten, Abwesenheiten, Kalenderzuordnung
Kunden- und Termindaten	Termine, Leistungen, Produkte, Ressourcen, Status, Präferenzen und notwendige Terminhinweise

Abrechnungs- und Geschäftsdaten	Rechnungsempfänger, Rechnungspositionen, Preise, Steuerangaben, Zahlungsart und Zahlungsstatus; keine vollständigen Zahlungskartendaten
Kommunikations- und Supportdaten	Einladungen, Service-E-Mails, Supportanfragen und angewiesene Kommunikation
Profil- und Mediendaten	Studio- und Profiltexthe, Kontaktdaten, Logos und Profilbilder
Nutzungs-, Sicherheits- und Protokolldaten	Zeitpunkte, technische Kennungen, Benutzer-/Studio-ID, Rollenänderungen, IP-Adresse in Infrastrukturprotokollen
Freitextdaten	Kundennotizen, Terminnotizen, Aufgabenbeschreibungen und sonstige vom Kunden eingegebene Inhalte

5. Besondere Kategorien personenbezogener Daten

Bedingte Verarbeitung. Gesundheitsdaten wie Allergien, Unverträglichkeiten, Hautempfindlichkeiten, Erkrankungen, Schwangerschaft oder behandlungsrelevante Hinweise können verarbeitet werden, wenn der Kunde sie gezielt und rechtmäßig eingibt. Betty & June Digital verwendet diese über missbettyjune.com verarbeiteten Angaben nicht für eigene Werbung, Profilbildung oder Datenhandel.

6. Häufigkeit und Dauer

Die Verarbeitung erfolgt fortlaufend während der Nutzung. Die Dauer richtet sich nach dem Hauptvertrag, der Speicherung in einem Free-Status und den Löschfristen in § 10 sowie Anlage 4.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Der Kunde genehmigt die nachstehend aufgeführten Unterauftragsverarbeiter allgemein. Die Liste wird nach § 11 aktuell gehalten.

Anbieter / Sitz	Leistung	Verarbeitung / Garantien
Hetzner Online GmbH Industriestraße 25 91710 Gunzenhausen Deutschland	Serverhosting, Rechenzentrum, Netzwerk; getrenntes verschlüsseltes Backupziel	Produktivverarbeitung und Speicherung in Deutschland. Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO. Datenbank und Dateien liegen auf der von Betty & June Digital für missbettyjune.com betriebenen Infrastruktur.
Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown, Dublin 18 Irland	Microsoft 365, Exchange Online und Microsoft Graph für transaktionalen E-Mail-Versand, unter anderem Terminerinnerungen und Systembenachrichtigungen	Verarbeitung nach Microsoft Products and Services Data Protection Addendum. 90 Tage Aufbewahrung in „Gesendete Elemente“. Weitere Microsoft-Unterauftragnehmer und mögliche internationale Zugriffe nach aktueller Microsoft-Dokumentation; Garantien nach Kapitel V DSGVO, insbesondere EU- Standardvertragsklauseln (vgl. § 12 Absatz 4).

Aktuelle Nachweisquellen

- Hetzner AVV/DPA: https://www.hetzner.com/AV/DPA_de.pdf
- Microsoft Products and Services Data Protection Addendum: <https://aka.ms/DPA>
- Microsoft-Unterauftragnehmerliste: <https://aka.ms/subprocessor>
- Status des EU-US Data Privacy Framework: <https://www.dataprivacyframework.gov/>

Anlage 3 – Technische und organisatorische Maßnahmen

Die nachfolgenden Maßnahmen beschreiben das vereinbarte Schutzniveau. Sie sind risikoorientiert anzuwenden und regelmäßig auf Wirksamkeit zu überprüfen.

1. Organisation und Vertraulichkeit

- Dokumentierte Verantwortlichkeit bei Betty & June Digital und zentraler Datenschutzkontakt unter hello@bettyjunedigital.com.
- Zugriff auf Produktivsysteme nur für ausdrücklich autorisierte und auf Vertraulichkeit verpflichtete Personen.
- Need-to-know- und Least-Privilege-Prinzip; regelmäßige Überprüfung und unverzüglicher Entzug nicht mehr benötigter Rechte.
- Datenschutz- und Sicherheitsanforderungen werden bei Änderungen an Personal, Dienstleistern oder Systemen neu bewertet.

2. Zutritts- und physischer Schutz

- Betrieb in einem Rechenzentrum von Hetzner in Deutschland; physische Zutrittskontrollen liegen im Verantwortungsbereich des vertraglich gebundenen Rechenzentrumsanbieters.
- Keine lokale Speicherung der Produktivdaten in öffentlich zugänglichen Geschäftsräumen.
- Administrative Endgeräte sind durch Festplattenverschlüsselung und automatische Bildschirmsperre geschützt.

3. Zugangs- und Authentifizierungsschutz

- Serveradministration über persönliche SSH-Schlüssel; kein regulärer Passwortzugriff auf SSH.
- Mehrfaktor-Authentifizierung für Hetzner, GitHub und Microsoft 365.
- Passwörter der Benutzer von missbettyjune.com werden mit einem geeigneten adaptiven Passwort-Hashverfahren gespeichert; Klartextpasswörter werden nicht gespeichert.
- Passwort-Reset- und Kontoeinrichtungslinks verwenden zufällige Einmaltokens; in der Datenbank werden nur kryptografische Token-Hashes gespeichert.
- Loginversuche werden nach E-Mail- und IP-bezogenen Grenzwerten begrenzt; E-Mail und IP werden für die persistente Drosselung nur als HMAC-Hash gespeichert.

4. Zugriffs- und Mandantentrennung

- Rollen- und berechtigungsbasierte Zugriffskontrolle auf Account-, Team-, Studio- und Kalenderfunktionen.
- Mandantenzuordnung über Studio- und Teamkontext; serverseitige Berechtigungsprüfung vor Datenzugriffen.
- Datenbankbeziehungen und Integritätsprüfungen unterstützen die Trennung von Studiodaten; Laufzeit- und Migrationsrollen der Datenbank sind getrennt.
- Die Datenbank ist nicht direkt aus dem öffentlichen Internet erreichbar; Anwendungszugriff erfolgt über den geschützten Serverprozess.

5. Übertragungs- und Kommunikationsschutz

- Öffentliche Verbindungen zur App erfolgen über HTTPS/TLS; die Anwendung ist nur hinter einem kontrollierten Reverse Proxy erreichbar.
- E-Mail-Übergabe an Microsoft Graph erfolgt verschlüsselt über HTTPS auf Port 443 und ist auf ein festgelegtes Absenderpostfach begrenzt.
- Produktivgeheimnisse werden außerhalb des Quellcodes in zugriffsbeschränkten Umgebungs- oder Secret-Dateien gespeichert.
- Keine vollständigen Zahlungskartendaten in missbettyjune.com; die eigene SaaS-Abrechnung erfolgt über Stripe außerhalb der fachlichen Studio-Auftragsdaten.

6. Datei- und Medienverarbeitung

- Uploadtypen, Dateisignaturen und Größen werden serverseitig validiert.
- Profilbilder werden auf ein festgelegtes WebP-Format und eine begrenzte Auflösung transformiert; Metadaten und Originaldateien werden nicht dauerhaft übernommen.
- Dateien erhalten servergenerierte Namen und restriktive Dateirechte; der Zugriff erfolgt über kontrollierte Anwendungsrouten.

7. Protokollierung und Nachvollziehbarkeit

- Anwendungsprotokolle vermeiden Anfrageinhalte, Passwörter, Tokens und Gesundheitsdaten; Fehler werden auf sichere Codes und technische Metadaten begrenzt.
- Nginx- und Systemprotokolle werden grundsätzlich 30 Tage aufbewahrt und anschließend rotiert oder gelöscht.
- Sicherheits- und Auditprotokolle werden grundsätzlich 12 Monate aufbewahrt. Vorfallsbezogene Auszüge dürfen bis zur abschließenden Klärung gesperrt bleiben.
- Zugriff auf Protokolle ist auf Administration und Sicherheitsanalyse beschränkt.

8. Verfügbarkeit, Sicherung und Wiederherstellung

- Tägliche verschlüsselte Sicherung auf ein vom Produktivserver getrenntes Backupziel bei Hetzner in Deutschland.
- Backup-Rotation von 30 Tagen; Sicherungen sind gegen allgemeinen Anwendungszugriff getrennt und zugriffsbeschränkt.
- Regelmäßige sowie nach wesentlichen Änderungen durchgeführte Wiederherstellungsproben; Ergebnisse werden dokumentiert.
- Datenbank und Dateien werden als logisch zusammengehöriger Sicherungssatz behandelt; Integritätsprüfungen unterstützen einen konsistenten Restore.

9. Löschung und Datenminimierung

- Kontrollierte Lösch- und Anonymisierungsfunktionen für Kunden- und Kontodaten; relationale Löschregeln verhindern unkontrollierte Restbestände.

- Produktivdaten werden nach Vertragsende gemäß § 10 gelöscht; Backups folgen der 30-tägigen Rotation.
- Microsoft-365-Kopien in „Gesendete Elemente“ werden grundsätzlich nach 90 Tagen automatisch gelöscht.
- Freitext- und Profelfelder besitzen Größenbegrenzungen; unnötige Originalbilder und Bildmetadaten werden verworfen.

10. Sichere Entwicklung und Prüfung

- Quellcodeverwaltung mit persönlichen Konten und Mehrfaktor-Authentifizierung; keine Produktivgeheimnisse im Repository.
- Automatisierte Unit-, Integrations- und relevante End-to-End-Tests für Berechtigungen, Mandantentrennung, Authentifizierung und Löschvorgänge.
- Kontrollierte Datenbankmigrationen mit getrennten Rollen und Prüfungen vor dem Produktiveinsatz.
- Sicherheitsrelevante Abhängigkeiten und Betriebsdokumentation werden im Rahmen von Wartung und Releases überprüft.

11. Vorfalls- und Kontinuitätsmanagement

- Definierter Datenschutzkontakt und unverzügliche Eskalation erkannter Vorfälle.
- Erstinformation des Kunden möglichst innerhalb von 24 Stunden; nachgelagerte Ergänzung verfügbarer Informationen.
- Sicherung relevanter Beweise ohne unnötige Offenlegung personenbezogener Daten; Abhilfemaßnahmen und Lessons Learned werden dokumentiert.

Anlage 4 – Lösch- und Aufbewahrungskonzept

Datenbestand	Regelfrist / Ereignis	Maßnahme
Aktive Studio-, Kunden-, Termin- und Mitarbeiterdaten	Während der Vertrags- und Speicherdauer	Verarbeitung nach Weisung und Nutzung durch den Kunden
Übergangs- und Exportphase nach vollständiger Beendigung	30 Tage	Nur Rückgabe, Export, Sicherung und erforderliche Administration; keine neue fachliche Nutzung
Produktivdaten nach Übergangsphase	Löschung innerhalb weiterer 30 Tage	Löschen oder geeignete Anonymisierung; gesetzliche Daten werden gesperrt
Getrennte Backups	30-tägige Rotation	Automatisches Überschreiben/Löschen; bei Restore erneute Anwendung der Löschprozesse
Microsoft 365 – Gesendete Elemente	90 Tage	Automatische Löschung; Ausnahmen nur bei dokumentierter Aufbewahrungssperre
Nginx- und Systemprotokolle	30 Tage	Rotation oder Löschung; vorfallsbezogene Sicherung möglich
Sicherheits- und Auditprotokolle	12 Monate	Automatische Löschung; längere Sperrung nur zur Vorfallklärung oder bei Rechtsansprüchen
Login-Drosselungsdaten	Ablauf des jeweiligen Schutzfensters	Automatisches Cleanup; nur HMAC-Hashes statt Klartext-E-Mail/IP
Passwort-Reset- und Einrichtungstokens	30 Minuten bzw. 24 Stunden sowie nach Verwendung	Token ist einmalig; Datenbank enthält nur Hash; abgelaufene Einträge werden bereinigt
Profilbilder	Bis Austausch, Entfernung oder maßgeblicher Kontolöschung	Alte Datei wird nach erfolgreichem Austausch entfernt; Original und Metadaten werden nicht gespeichert
Gesetzlich aufzubewahrende Daten	Nach anwendbarer gesetzlicher Frist	Sperrung und ausschließliche Verarbeitung zum gesetzlichen Zweck