

Auftragsverarbeitungsvereinbarung nach Art 28 DSGVO

zwischen

Dualbrief Kunde

- im folgenden „Auftraggeber“ genannt –

und

KMH Management GmbH & Co. KG

Winterhäuser Str. 87D

97084 Würzburg

- im folgenden „Auftragnehmer“ genannt –

Dokumenteninformationen

Zweck und Gültigkeit

Auftraggeber und Auftragnehmer stehen unmittelbar vor Abschluss eines Hauptvertrags betreffend einer gemeinsamen Partnerschaft.

In folgender Auftragsverarbeitungsvereinbarung sind jene vom Auftragsverarbeiter einzuhaltende Bestimmungen gemäß der DSGVO festgelegt. Sonstige vertragliche Pflichten aus dem Hauptvertrag bleiben von dieser Vereinbarung unberührt.

Dieses Dokument ist mit dem Datum der Freigabe (siehe „Status“ im Kapitel „Dokumentenhistorie“) auf unbefristete Zeit gültig. Eine freigegebene Fassung mit einer höheren Versionsnummer beendet die Gültigkeit dieses Dokuments.

Verteilerliste

Name	Organisation	Position	E-Mail Adresse
Michael Kunter	KMH Management GmbH & Co. KG	Geschäftsführung	michael.kunter@kmh-management.de
Kai Ubben	KMH Management GmbH & Co. KG	Geschäftsführung	kai.ubben@kmh-management.de
	Auftraggeber		

Dokumentenhistorie

Version	Status	Datum	Erstellt & geprüft	Freigegeben	Änderungsgrund
V1.0	Freigegeben	04.03.2026	Kai Ubben	KU	Initial-Erstellung

Copyright/ Vertraulichkeit

Die vorliegenden elektronischen Unterlagen und Dateien wurden von KMH Management erstellt und enthalten keine urheberrechtlichen geschützten Inhalte Dritter. Eine Vervielfältigung, Weitergabe oder sonstige Nutzung – ganz oder in Teilen – ist ohne vorherige schriftliche Zustimmung der Autoren untersagt. Sämtliche enthaltenen Informationen stellen Geschäftsgeheimnisse sowie vertrauliche, technische oder kommerzielle Daten dar. Sie werden ausschließlich zu Prüfzwecken zur Verfügung gestellt und dürfen ohne ausdrückliche Genehmigung der oben genannten Firmen nicht offengelegt oder anderweitig verwendet werden.

1. Gegenstand der Vereinbarung

- 1) Der Inhalt der vom Auftragnehmer zu erbringenden Leistungen ist im Hauptvertrag festgelegt.
- 2) Der Auftragnehmer darf aufgrund dieser Vereinbarung verarbeiteten personenbezogenen Daten nur im Rahmen der Vertragserfüllung und gemäß den Anforderungen und Weisungen des Auftraggebers sammeln, verarbeiten und nutzen.
- 3) Diese Vereinbarung ist als Ergänzung zu unseren bestehenden Verträgen zu verstehen.
- 4) Die datenschutzrechtlich relevante Datenverarbeitung bezieht sich auf die Nutzung des Produkts **„DIKKI“, DU@LBRIEF (Postausgang), Dokumentenmanagement und Postausgang**. Dazu gehören auch die Verwendung der personenbezogenen Daten im Zuge der elektronischen Zustellung, die Erbringung postalischer Sendungen sowie die Bearbeitung von damit verbundenen Supportfällen.
- 5) Im Zuge des Auftrags werden vom Auftragnehmer folgende Datenkategorien verarbeitet: Namensdaten, Adressdaten, Kontaktdaten, Vertragsdaten,

Verrechnungsdaten, Rückscheindaten, Inhaltsdaten (Dokumenteninhalt, Schriftverkehr), Bilddaten aus Scans, Aktenzeichen, Klassifizierungsmerkmale.

6) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Empfänger der Sendung (z.B.: Kunde, Bürger, Interessent, Mitglied, Partner, Mitarbeiter des Auftraggebers sowie Geschäftspartner, deren Dokumente verarbeitet werden).

7) Jede nicht durch diese Vereinbarung gedeckte Datenverarbeitung und -Übermittlung durch den Auftragnehmer bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

2. Pflichten des Auftragnehmers

1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag zur Herausgabe von Daten des Auftraggebers, so hat er – soweit rechtlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Eine Verarbeitung der Daten zu anderen Zwecken als der „Dualen Zustellung“ und den damit verbundenen Tätigkeiten des Auftragnehmers bedarf eines gesonderten schriftlichen Auftrags. Dies gilt ebenso für alle im Rahmen von **DIKKI** und **DU@LBRIEF** erbrachten Leistungen, insbesondere bei der Posteingangsbearbeitung sowie der Digitalisierung von Dokumenten und Akten. Der Auftragnehmer speichert die hierbei verarbeiteten personenbezogenen Daten und Dokumenteninhalte ausschließlich für die Dauer des Bearbeitungsprozesses, übergibt diese an den Auftraggeber und löscht oder vernichtet sie anschließend nach den vereinbarten Fristen.

2) Der Auftragnehmer sichert rechtsverbindlich zu, dass alle mit der Datenverarbeitung betrauten Personen vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit verpflichtet wurden oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung bleibt auch nach Beendigung der Tätigkeit und dem Ausscheiden beim Auftragnehmer bestehen.

3) Der Auftragnehmer erklärt, alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO ergriffen zu haben (Einzelheiten siehe Anlage /1). Zudem verpflichtet er sich, die Grundsätze der Datenverarbeitung gemäß Art. 5 sowie die Vorgaben zur datenschutzfreundlichen Technikgestaltung nach Art. 25 DSGVO einzuhalten.

4) Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen, damit der Auftraggeber die Rechte betroffener Personen nach Kapitel III DSGVO (Information, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann. Hierfür stellt der Auftragnehmer dem Auftraggeber alle notwendigen Informationen bereit. Geht

beim Auftragnehmer ein Antrag ein, der erkennbar irrtümlich an ihn statt an den Auftraggeber gerichtet ist, leitet der Auftragnehmer diesen unverzüglich an den Auftraggeber weiter und informiert den Antragsteller darüber.

5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere in Bezug auf Datensicherheitsmaßnahmen, Meldungen von Datenschutzverletzungen, Benachrichtigung betroffener Personen, Datenschutz-Folgeabschätzungen sowie erforderliche Konsultationen mit Aufsichtsbehörden.

6) Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 DSGVO für die vorliegende Auftragsverarbeitung zu führen.

7) Dem Auftraggeber wird das Recht eingeräumt, jederzeit Einsicht in die Verarbeitung der überlassenen Daten zu nehmen und diese zu kontrollieren, auch durch von ihm beauftragte Dritte. Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle Informationen zur Verfügung zu stellen, die für die Überprüfung der Einhaltung dieser Vereinbarung erforderlich sind.

8) Nach Beendigung dieser Vereinbarung hat der Auftragnehmer sämtliche Verarbeitungsergebnisse und Unterlagen mit personenbezogenen Daten an den Auftraggeber zu übergeben oder auf dessen Weisung hin zu vernichten. Werden die Daten in einem speziellen technischen Format verarbeitet, ist der Auftragnehmer verpflichtet, diese in diesem Format herauszugeben.

9) Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt.

10) Der Auftragnehmer verpflichtet sich, die vom Auftraggeber übergebenen Daten für Zwecke der Verrechnung, Reklamation, des Supports und weiterer notwendiger Tätigkeiten bis zu 90 (neunzig) Tage aufzubewahren und die Daten nach Ablauf dieser Frist zu löschen oder zu vernichten.

11) Der Auftragnehmer sichert zu, dass alle mit der Datenverarbeitung und -übermittlung betrauten Arbeitnehmer vor Aufnahme ihrer Tätigkeit zur Wahrung des Datengeheimnisses gemäß § 53 BDSG verpflichtet wurden. Diese Verpflichtung besteht auch nach Beendigung des Arbeitsverhältnisses fort.

12) Soweit rechtlich erforderlich, bestellt der Auftragnehmer einen Datenschutzbeauftragten und teilt dem Auftraggeber dessen Kontaktdaten mit.

3. Ort der Durchführung der Datenvereinbarung

Alle Verarbeitungstätigkeiten personenbezogener Daten, einschließlich der Scan- und Archivierungsprozesse im Rahmen von DIKKI und DU@LBRIEF, finden ausschließlich auf dem Gebiet der Europäischen Union statt.

4. Sub-Auftragsverarbeiter

- 1) Der Auftragnehmer ist berechtigt, Sub-Auftragsverarbeiter für Tätigkeiten im Zusammenhang mit dem Produkt „DIKKI“ und DU@LBRIEF einzusetzen. Dies umfasst insbesondere den Ausdruck, die Kuvertierung und Postaufgabe, das Einscannen von Rückscheininformationen, den Betrieb der Systeme in einem Rechenzentrum sowie die Posteingangsbearbeitung und die Digitalisierung von Dokumenten und Akten
- 2) Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor der Einbindung eines Sub-Auftragsverarbeiters, sodass dieser die Möglichkeit hat, den Einsatz zu untersagen.
- 3) Mit jedem Sub-Auftragsverarbeiter schließt der Auftragnehmer eine Vereinbarung im Sinne von Art. 28 Abs. 4 DSGVO ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter denselben Pflichten unterliegt, die auch dem Auftragnehmer aus dieser Vereinbarung erwachsen.
- 4) Verstößt ein Sub-Auftragsverarbeiter gegen seine datenschutzrechtlichen Verpflichtungen, haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.
- 5) Die jeweils genehmigten Sub-Auftragsverarbeiter sind in Punkt 7 der Anlage 2 aufzuführen.

5. Unterschriften

Auftraggeber:

Ort, Datum:

Unterschrift

Auftragnehmer:

Würzburg, Datum

Unterschrift:

Anlage 1

Technisch und organisatorische Maßnahmen

Ergänzend für das Produkt „DIKKI“: Bei der physischen und digitalen Verarbeitung von Dokumenten werden zusätzliche Schutzmaßnahmen umgesetzt. Dazu zählen insbesondere: Zutrittskontrolle zu Scan- und Posteingangsräumen, dokumentierte Übergabeprozesse, Protokollierung von Scanvorgängen, verschlüsselte Speicherung digitaler Abbilder, sichere Vernichtung von Papieroriginalen, soweit vereinbart, sowie organisatorische Maßnahmen zur Trennung verschiedener Auftraggeber.

Die KMH Management GmbH & Co. KG richtet ihre Prozesse und Verfahren an den Vorgaben der Normen ISO 9001 und ISO 14001 aus.

Im Folgenden werden beispielhaft die umgesetzten technischen und organisatorischen Maßnahmen gemäß DSGVO aufgeführt.

1. Vertraulichkeit

- Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen (z. B. Schlüssel, Chipkarten, Türsysteme, Sicherheitspersonal, Alarm- und Videoanlagen).
- Zugangskontrolle: Schutz vor unbefugter Systemnutzung (z. B. Passwort-Policy, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern).
- Zugriffskontrolle: Verhinderung unbefugten Lesens, Kopierens, Veränderns oder Löschens (z. B. Berechtigungen nach „Need-to-know“, standardisierte Prozesse, Protokollierung, regelmäßige Überprüfung – insbesondere administrativer Konten).
- Pseudonymisierung: Trennung bzw. Entfernung von Identifikationsmerkmalen personenbezogener Daten, sofern möglich.
- Datenklassifizierung: Einstufung von Daten nach gesetzlichen Vorgaben oder internen Regelungen (z. B. „vertraulich / intern / öffentlich“).

2. Integrität

- Weitergabekontrolle: Sicherstellung, dass personenbezogene Daten bei elektronischer Übertragung, Transport oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (z. B. Verschlüsselung, VPN, Protokollierung).
- Eingabekontrolle: Nachvollziehbarkeit und Dokumentation, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt

wurden (z. B. Protokollierung, eindeutige Benutzerkennungen, Vier-Augen-Prinzip).

3. Verfügbarkeit

- Verfügbarkeitskontrolle: Schutz vor zufälliger oder vorsätzlicher Zerstörung bzw. Verlust (z. B. unterbrechungsfreie Stromversorgung, Klimatisierung, Firewalls, Virenschutz, Backups, Notfallpläne).
- Wiederherstellbarkeit: Sicherstellung, dass Systeme und Daten bei einem technischen Zwischenfall zeitnah wiederhergestellt werden können (z. B. Datensicherung, Disaster-Recovery-Konzept, regelmäßige Tests der Wiederherstellung).

4. Belastbarkeit

- Belastbarkeit der Systeme: Einsatz geeigneter Maßnahmen, um eine dauerhafte Funktionsfähigkeit und Ausfallsicherheit von Systemen und Diensten zu gewährleisten (z. B. Monitoring, Redundanz, Lastverteilung, Notfallübungen).

5. Verfahren zur regelmäßigen Überprüfung

- Kontroll- und Evaluationsprozesse: Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (z. B. interne Audits, externe Prüfungen, Penetrationstests, kontinuierliche Verbesserungsprozesse).

Anlage 2

Genehmigte Subunternehmer

Der Auftraggeber erteilt hiermit seine Zustimmung zum Einsatz folgender weiterer Auftragsverarbeiter:

Subunternehmer	Verarbeitungsstandort	Art der Dienstleistung
hpc DUAL Holding GmbH	Hasnerstr. 123, 1160 Wien, Deutschland	Datenverarbeitung, digitale Zustellung
FP Document Services GmbH	Trebuser Straße 47/Haus 1, 15517 Fürstenwalde/Spree, Deutschland	Weboberfläche & Software (Druckertreiberlösung) zur Datenübernahme
Business Unit Campaign direct services Gütersloh GmbH	Reinhard-Mohn-Str. 300 33333 Gütersloh	Physische Druckdienstleistung, Versandaufbereitung, Versand der Dokumente
CodX Software AG	Sinserstr. 47. 6330 Cham, Schweiz	Datenverarbeitung Posteingangsscan
Infoscan GmbH	Oberer Renngrund 8, 74889 Sinsheim-Reihen	Datenverarbeitung Dokumentenscan