

Vertrag Datennutzung Klink

Version 1.0.0., Stand: 21.11.2022

Datennutzungsvertrag

zwischen

der natürlichen Person
Könighaus Klink GbR

– nachfolgend: Klink –

und

dem Vertragspartner

– nachfolgend: Datengebende Stelle –

wird in Hinblick auf die im **Anhang Datenbasis** genannten Datenbestände

– Vertragsgegenstand, Datenbasis –

folgender Datennutzungsvertrag geschlossen:

§ 1 Hauptpflichten

a) Einräumung von Nutzungsrechten

- (1) Die Datengebende Stelle räumt Klink das Recht ein, die Datenbasis in eigener datenschutzrechtlicher Verantwortlichkeit und unter Einhaltung aller einschlägigen Rechtsvorschriften zu nutzen. Die Nutzungsrechte sind nicht übertragbar und nicht ausschließlich. Der Umfang der Nutzungsrechte ergibt sich im Übrigen aus den nachfolgenden Bestimmungen

b) Zugänglichmachung der Datenbasis

- (1) Die Datengebende Stelle verpflichtet sich Klink die Datenbasis gemäß der im **Anhang Datenzugang** genannten beschriebenen Vorgehensweise zugänglich zu machen.

c) Verantwortliche Datenverarbeitung durch Klink

- (1) Klink verpflichtet sich, die Datenbasis in eigenem Namen und in eigener datenschutzrechtlicher Verantwortlichkeit zu verarbeiten. Sie geben dabei den schutzwürdigen Interessen von Personen, die von der Verarbeitung betroffen sind, im Zweifel Vorrang gegenüber eigenen Interessen. Sie kennen die neben diesem Vertrag anwendbaren rechtlichen Bestimmungen und halten sie ein und sich darüber im Klaren, dass eine Nichteinhaltung ggf. auch strafrechtliche Konsequenzen haben kann

§ 2 Datenbasis

- (1) Die Erläuterungen zum Umfang der Datenbasis, sowie dessen Pflege und Zugänglichmachung werden im **Anhang Datenbasis, -pflege und -zugang** genannt.

§ 3 Verarbeitungszweck

- (1) Klink verpflichtet sich die Datenbasis ausschließlich zu den im **Anhang Datenbasis, -pflege und -zugang** beschriebenen Zwecken zu nutzen und unterliegt diesbezüglich einer datenschutzrechtlichen Zweckbeschränkung.
- (2) Ohne ausdrückliches schriftliches Einverständnis des Datengebers dürfen keine Patente oder andere gewerblichen Schutzrechte, die sich auf die Daten beziehen oder durch diese begründet werden, angemeldet werden.

§ 4 Nutzungsdauer

a) Reguläre Dauer der Nutzungsberechtigung

- (1) Die vorgenannten Nutzungsrechte werden unbefristet eingeräumt.

b) Vorzeitiges Kündigungsrecht der Datengebenden Stelle

- (1) Der Nutzungsberechtigung kann von der Datengebenden Stelle vorzeitig ohne Angabe von Gründen mit einer Frist von 4 Wochen gekündigt werden.
- (2) Der Nutzungsberechtigung kann von der Datengebenden Stelle unter Bestimmung einer angemessenen Frist vorzeitig gekündigt werden, wenn sie ihrerseits zur Veranlassung der Löschung der Datenbasis verpflichtet ist. Sie soll sich in diesem Fall aktiv darum bemühen, den durch die Löschung entstehenden Schaden für die anderen Vertragsparteien so gering wie möglich zu halten.

c) Ende der Nutzungsberechtigung bei Auflösung oder Änderung des Zwecks des Gewerbes

- (1) Klink verpflichtet sich, die Datengebenden Stellen unverzüglich, spätestens innerhalb von 14 Tagen, in Kenntnis zu setzen.

- (2) Die Änderung ist durch Ergänzung des Anhangs zu dokumentieren. Sie ist nicht zustimmungspflichtig.
- (3) Das Nutzungsrecht endet, sofern das Klink sich auflöst oder der Zweck des Gewerbes sich grundlegend von dem im Anhang beschriebenen Vorhaben ändert. In diesem Fall sollen die Parteien versuchen einen neuen Vertrag abzuschließen, sofern seitens Klink ein berechtigtes Interesse an der Weiternutzung besteht.

d) Kündigung durch Klink

- (1) Die auf sie bezogene Nutzungsberechtigung kann von Klink ordentlich mit zwei Wochen Kündigungsfrist zum Monatsende gekündigt werden.

§ 5 Datenschutzrechtliche Pflichten und Garantien

a) Zweckbeschränkung

- (1) Klink verwendet die Datenbasis ausschließlich zu den in diesem Vertrag und seinen Anhängen spezifizierten Zwecken, vgl. § 2.

b) Transparenz

- (1) Alle Vertragsparteien verpflichten sich zur Einhaltung der für sie geltenden gesetzlichen Transparenzvorgaben bezüglich der Datenverarbeitungen, die Gegenstand dieses Vertrags sind. Auf Art 12 ff. DSGVO wird hingewiesen.
- (2) Die Notwendigkeit der Speicherung der personenbezogenen Nutzerdaten bei Klink zu Zwecken der Kommunikation, Betreuung sowie zur Kontrolle der Nutzungsverträge und für die Einhaltung von Rechenschaftspflichten ist bekannt.
- (3) Darüber hinaus können die von der Datengebenden Stelle im Rahmen des Vertragsverhältnisses gemachten Angaben, einschließlich der personenbezogenen Daten, seitens Klink über das Vertragsende hinaus für statistische Zwecke, an denen insoweit ein berechtigtes Interesse besteht, gespeichert werden. Hiergegen besteht ein Widerspruchsrecht.
- (4) Bezüglich der Speicherung der Daten durch Klink besteht ein Auskunftsanspruch, sowie ggf. ein Korrektur-, und Löschanpruch, sowie ein Recht auf Datenübertragbarkeit.

c) Richtigkeit und Datenminimierung

- (1) Die Datengebende Stelle und das Klink verpflichten sich, die Aufbereitung, Anonymisierung und Überlassung der Datenbasis mit der üblichen und angemessenen Sorgfalt durchzuführen, übernimmt jedoch keine Gewährleistung für deren Fehlerfreiheit.
- (2) Klink ist verpflichtet, potenzielle Fehler oder Mängel in der Datenbasis der Datengebenden Stelle mitzuteilen. Die Datengebenden Stelle ist berechtigt Hinweise auf Mängel in die eigene Datendokumentation aufzunehmen. Dabei sind die berechtigten Interessen von Klink zu beachten.
- (3) Bei gravierenden Mängeln, soll der Datengebenden Stelle eine angemessene Frist zur Beseitigung der Mängel eingeräumt werden. Wenn eine Mängelbeseitigung nicht mehr zu erwarten ist, darf Klink vom Vertrag zurücktreten. Dieser Rücktritt hat die Wirkung, dass eventuell bereits gezahlte Entgelte zurückzugewähren sind und das Nutzungsrecht endet.

d) Dauer / Speicherbegrenzung

- (1) Klink ist zur Löschung der Datenbasis zum Ende der vereinbarten Nutzungsdauer innerhalb von 4 Wochen verpflichtet. Diese Pflicht erstreckt sich auch auf sämtliche Teile der Datenbasis sowie auf Sicherungskopien, modifizierte Kopien, Auszugsdateien, Hilfsdateien und Ausdrucke der Datenbasis (im Folgenden Derivate).
- (2) Ausgenommen von der Löschpflicht sind solche Daten und Derivate, die kein Risiko für betroffene Personen mit sich bringen oder die keine Personenbeziehbarkeit mehr aufweisen – dies gilt regelmäßig erst dann, wenn auch einer Veröffentlichung dieser Daten keine Bedenken entgegenstünden.

- (3) Sofern die Datengebende Stelle zur Veranlassung der Löschung der Datenbasis durch Klink rechtlich verpflichtet ist, muss Klink die Löschung durchführen. Das Gleiche gilt, sofern sie gegenüber dem Betroffenen direkt verpflichtet sind.

e) Sicherheit der Datenverarbeitung

- (1) Die Datennutzenden verpflichten sich stets ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau einzuhalten. Dies geschieht in der Regel durch Einhaltung der im Anhang Technische- und organisatorische Maßnahmen beschriebenen Maßnahmen. Diese soll durch die Parteien einvernehmlich an den jeweiligen technischen Fortschritt angepasst werden. Sofern ein konkreter Bedarfsfall besteht, haben alle Parteien auch über die im vorgenannten Anhang erwähnten Maßnahmen hinaus eigenständig weitere Maßnahmen zu ergreifen.

f) Besondere Kategorien von Daten

- (1) Sofern die Datenbasis besonderer Kategorien von Daten im Sinne von Art. 9 DSGVO enthält, wird den besonderen Schutzanforderungen für die Verarbeitung durch die im Anhang Technische- und organisatorische Maßnahmen beschriebenen Schutzmaßnahmen Rechnung getragen, die insoweit der Sensibilität der Daten angepasst sind und ihr in besonderer Weise Rechnung tragen.

g) Beschränkung der Zugriffsberechtigten, Weiterübermittlung

- (1) Ein Zugriff auf die Datenbasis ist grundsätzlich nur für Klink gestattet. Klink ist es nicht gestattet, sich bei der Haltung, Verarbeitung oder Nutzung der Datenbasis der Hilfe Dritter (Auftragnehmer, Selbständige, freiberuflich Tätige) zu bedienen; der Abschluss von einvernehmlichen Auftragsvertragsverträgen wird dadurch nicht berührt.
- (2) Klink sichert zu, die Datenbasis und alle Kopien der Datenbasis geheim zu halten. Dieses Datengeheimnis besteht auch nach dem Ende der vereinbarten Nutzungsdauer fort.
- (3) Mitarbeitende von Klink können Zugriff zu der Datenbasis und der Derivate erhalten, sofern sie durch schriftliche Vereinbarung der Einhaltung der Pflichten zugestimmt haben.

h) Auftragsverarbeitungen

- (1) Klink darf weitere Auftragsvertragsverträge mit Dritten abschließen, sofern sie der DSGVO entsprechen.

i) Drittbegünstigung und Rechte betroffener Personen

- (1) Allen von der Verarbeitung durch Klink betroffenen Personen werden gegenüber Klink mindestens die gleichen Rechte, wie sie aus gesetzlichen Bestimmungen gegenüber den Datengebenden Stellen bestehen, eingeräumt.

j) Internationale Datenübermittlungen

- (1) Die Verarbeitung der Datenbasis ist in allen Mitgliedstaaten der Europäischen Union sowie allen Staaten für die die Europäische Kommission nach Art. 45 Abs. 1 DSGVO die Angemessenheit des Datenschutzniveaus festgestellt hat, gestattet.
- (2) Die Übermittlung in Drittstaaten und Verarbeitung der Datenbasis ist auf Grundlage und unter Einhaltung der EU-Standardvertragsklauseln, die diesem Vertrag als Anhang EU-Standardvertragsklauseln beigefügt ist, möglich. Die Regelungen dieser Vereinbarung gelten als Konkretisierungen der vorgenannten EU-Standardvertragsklauseln. Im Konfliktfall ist den Regeln der EU-Standardvertragsklauseln Vorrang einzuräumen.

§ 6 Vertragsverstöße und Haftung

a) Begriffsbestimmung

- (1) Verstöße gegen diesen Vertrag sind insbesondere:
- Die Verarbeitung oder Nutzung der Datenbasis zu anderen als den Zwecken dieses Vertrags
 - Die unzulässige Zugänglichmachung der Datenbasis oder Derivate an Dritte
 - Die Weitergabe von persönlichen Zugangscodes und Passwörtern
 - Der Verlust von Datenträgern, die die Datenbasis oder Derivate enthalten
 - Die Nichteinhaltung anderer im **Anhang Technische und organisatorische Maßnahmen** aufgelisteter Zusagen

b) Meldepflichten

- (1) Verstößt Klink gegen Verpflichtungen aus diesem Vertrag und insbesondere auch die Verpflichtung zur Einhaltung gesetzlicher Vorschriften, hat Klink die Datenschutzaufsichtsbehörden unverzüglich nach Kenntnisnahme zu informieren.

c) Fristlose Kündigung aus wichtigem Grund

- (1) Eine fristlose Kündigung aus wichtigem Grund kann insbesondere bei Vorliegen eines Vertragsverstoßes erfolgen.

d) Haftung

- (1) Die Datengebende Stelle haftet gegenüber Klink nicht für Verluste oder Schäden irgendwelcher Art im Zusammenhang mit den Vertragsdaten oder mit Schlussfolgerungen oder Empfehlungen, die in den übermittelten Daten enthalten sein können.
- (2) Die Datengebende Stelle haftet nur für vorsätzliches oder fahrlässiges Handeln; die Haftung für Folgeschäden ist ausgeschlossen. Bei fahrlässigem Handeln wird die Haftung auf vorhersehbare Schäden beschränkt.
- (3) Der Haftungsausschluss und die Haftungsbeschränkung gelten nicht bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, bei Schäden aus der Verletzung wesentlicher Vertragspflichten (sog. Kardinalpflichten) sowie bei der Haftung für zugesicherte Eigenschaften. Bei der Verletzung von Kardinalpflichten wird die Haftung für leichte Fahrlässigkeit auf vorhersehbare Schäden beschränkt. Eine Haftung für die Eignung der Datensätze für den von Klink intendierten Zweck wird nicht übernommen. Klink erkennt hiermit an, dass sie für die Folgen der Maßnahmen, die sie aufgrund der erhaltenen Daten oder als Ergebnis ihrer Interpretation der erhaltenen Daten treffen, allein verantwortlich sind.
- (4) Klink haftet für alle Schäden, die ihnen aus nicht vereinbarungsgemäßigem Umgang (fahrlässig oder vorsätzlich) im Rahmen der Überlassung der Datenbasis entstehen und stellt sie insoweit von Haftungsansprüchen Dritter frei. Die Ersatzpflicht entfällt, soweit Klink nachweisen kann, dass er die nach den Umständen des Falles gebotene Sorgfalt beachtet hat. Haftungsfälle berechtigen zur Kündigung aus wichtigem Grund. Die Geltendmachung weitergehender Ansprüche bleibt davon unberührt. Dies umfasst auch die Kosten einer angemessenen Rechtsverteidigung.

§ 7 Sonstiges

a) Änderungen/Teilunwirksamkeit

- (1) Änderungen dieses Vertrags sind nur gültig, wenn sie in Schriftform erfolgen; Anpassungen der Anhänge, wenn Sie in Textform erfolgen. Eine Partei kann von der anderen die Bestätigung der Änderung der Anhänge in Schriftform verlangen.

- (2) Sollte eine Bestimmung dieses Vertrags ungültig sein, so betrifft dies nicht den Vertrag als Ganzes. In einem solchen Falle ist der Vertrag seinem Sinn und Zweck entsprechend auszulegen, wobei zu berücksichtigen ist, was die Parteien gewollt hätten, wenn ihnen die Ungültigkeit einer Vertragsbestimmung bekannt gewesen wäre.

b) Anwendbares Recht

Es wird die Anwendung deutschen Rechts vereinbart. Ausschließlicher Gerichtsstand ist Dortmund.

Anhänge

Anhang Technische- und organisatorische Maßnahmen

a) Anwendungsbereich

- (1) Die nachfolgenden technischen und organisatorischen Maßnahmen gelten, sofern nicht für einzelne Auftragsverarbeiter oder Datennutzende in Hinblick auf die in ihrem Verarbeitungsbereich andere Maßnahmen spezifiziert wurden.

b) Management

- (1) Eine dem Risiko der Datenbasis angemessene Organisationsstruktur für die Informationssicherheit ist vorhanden und in die Prozesse und Abläufe integriert.
- (2) Alle Datennutzenden sowie ggf. alle weiteren Personen, die mit der Datenbasis in Kontakt kommen sind angemessen geschult und kennen insbesondere auch die Pflichten aus diesem Vertrag.
- (3) Die Datennutzenden stellen sicher, dass zur Datenbasis sowie zu Derivaten nur Personen Zugang haben, die unter entsprechender Anwendung des Verpflichtungsgesetzes verpflichtet wurden.

c) Anonymisierung, Pseudonymisierung und Datenminimierung

- (1) Die Datenbasis enthält unmittelbar personenbezogene Daten. Die Daten sind pseudonymisiert, wobei der unmittelbare Personenbezug über eine abgetrennte Verknüpfungstabelle hergestellt werden kann. Der Personenbezug des verbleibenden Datenbestands, also die Datenbasis – ohne die Pseudonyme – ist im o.g. Sinne anonymisiert/personenbezogen.
- (2) Eine dem Risiko der Datenbasis angemessene Organisationsstruktur für die Informationssicherheit ist vorhanden und in die Prozesse und Abläufe integriert.
- (3) Klink verpflichtet sich im Rahmen dieses Vertrages nur diejenigen Daten der Datenbasis zu verarbeiten, die sie benötigen
- (4) Jede Handlung, die darauf abzielt oder geeignet ist, die in den qualitativen Daten enthaltenen anonymisierten Informationen über Personen oder Organisationen zu deanonymisieren, ist zu unterlassen.

d) Verschlüsselung

- (1) Bei E-Mail, Messenger, Cloud-Plattformen erfolgt eine Transportverschlüsselung und eine Inhaltsverschlüsselung der Datenbasis und ihrer Derivate nach dem Stand der Technik. Bei Nutzung dieser Dienste ist durch die Art der Verschlüsselung sicher zu stellen, sodass auch der Dienstanbieter keine Entschlüsselung der Datenbasis oder ihrer Derivate vornehmen kann.

e) Vertraulichkeit

- (1) Klink verpflichtet sich auch in mündlichen Präsentationen oder Gesprächen mit Dritten keine personenbezogenen Informationen weiterzugeben, einschließlich solcher Informationen, die zur Re-Identifikation von Personen oder Organisationen führen können.

f) Verfügbarkeit

- (1) Der Zugang ist näher im **Anhang Datenbasis, -pflege und -zugang** beschrieben.

g) Regelmäßige Überprüfung

- (1) System- und Sicherheitstests wie z. B. Code-Scan und Penetrationstests, werden regelmäßig durchgeführt.

h) Autorisierung

- (1) Es werden starke Passwörter verwendet.
- (2) Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden.
- (3) Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetzte oder die IT-Abteilung) – im Ausnahmefall (z. B. längere Erkrankung) wird das Passwort durch die IT zurückgesetzt und dieser Vorgang dokumentiert.
- (4) Passwörter dürfen nicht auf Zettel oder Pinnwänden aufgezeichnet werden.
- (5) Keine Speicherung von Passwörtern im Browser ohne Sicherung durch ein Masterpasswort
- (6) Einsatz von Verfahren zur Zwei- oder Mehr-Faktor-Authentifizierung bei Verarbeitungstätigkeiten vor dem Zugriff auf die Datenbasis oder ihre Derivate (z. B. Chipkarten, Token)

i) Physische Sicherheit

- (1) Die Arbeitsmittel sind nach den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) abgesichert

j) Systemkonfiguration

- (1) Prüfung eingehender E-Mails mittels Anti-Malwareschutz
- (2) Software und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen
- (3) Die Datenbasis darf nur im Browser rezipiert werden. Nach dem Ende des Zugriffs auf Dokumente dürfen auf dem Computer des Benutzers keine Rückstände mehr bestehen, dies betrifft ausdrücklich auch alle temporären Speicherungen oder Zwischenspeicherungen etwa durch den Browser. Der Browser-Cache ist nach der Nutzung zu löschen.

k) Rechenschaftspflicht

- (1) Sicherheitsvorkommnisse werden konsequent dokumentiert.
- (2) Jede Erstellung von Kopien der Datenbasis (Derivate), die nicht nur temporär erstellt wird und mindestens am gleichen Arbeitstag gelöscht wird, ist durch Klink zu dokumentieren (mindestens: Dateiname, Speicherort und -datum). Die Dokumentation ist der Datengebenden Stelle auf Verlangen herauszugeben.
- (3) Die Löschung der Datenbasis und ihrer Derivate ist zu dokumentieren. Die Dokumentation ist der Datengebenden Stelle auf Verlangen herauszugeben. Die Löschung der Datenbasis und der Derivate bei Ende der Nutzungsrechte ist dem der Datengebenden Stelle durch Klink zu bestätigen.

l) Löschung

- (1) Die Löschung von Daten soll unter Beachtung der Vorgaben des BSI-Grundschutz-Kompendiums, CON.6: Löschen und Vernichten¹ erfolgen. Insbesondere ist bei der Löschung sicher zu stellen, dass die Daten nicht nur als gelöscht markiert wurden, sondern etwa durch Zufallswerte überschrieben wurden.
- (2) Für die Entsorgung und Vernichtung von Datenträgern und Papier ist DIN 66399 mindestens nach Klasse 2 (mindestens Sicherheitsstufe auf dem Niveau 3, i.e. P-4² für Papier, H-4³ für klassische Festplatten, E-4 für SSDs) der DIN 66399 einzuhalten.

¹ Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg): IT-Grundschutz-Kompendium, Stand: Februar 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehen_sweisen/CON_6_Loeschen_und_Vernichten_Edition_2021.pdf.

² Fläche der Materialteilchen max. 160 mm² und Breite des Streifens max. 6 mm.

³ Datenträger mehrfach zerteilt und verformt und Fläche der Materialteilchen max. 2000 mm².

Anhang Datenbasis, -pflege und -zugang

Die Datenbasis besteht zuallererst aus den allgemeinen Angaben des/der Inhaber/in der Datengebenden Stelle:

- Vorname
- Nachname
- vollständige Anschrift
- E-Mail-Adresse
- Telefonnummer
- und ähnliche

Anschließend erfolgen Angaben zur Datengebenden Stelle:

- Name
- vollständige Anschrift
- E-Mail-Adresse
- Telefonnummer
- Website
- Foto
- und ähnliche

Des Weiteren besteht die Datenbasis aus den Getränken und Speisen, die in der Datengebenden Stelle angeboten werden. Die Angaben zu den Getränken setzen sich dabei wie folgt zusammen:

- Name
- Marke
- Alkoholgehalt
- Beschreibung
- Preis
- Foto
- und ähnliche

Die Angaben zu den Speisen setzen sich dabei wie folgt zusammen:

- Name
- Beschreibung
- Preis
- Foto
- und ähnliche

Darüber hinaus besteht die Datenbasis aus weiteren Attributen der Datengebenden Stelle. Hierunter fallen:

- Happy Hour
- Öffnungszeiten
- Besondere Angebote (Kicker, Dartscheiben, Billard etc.)
- Ausstattung
- und ähnliche

- Die Pflege, Korrektur und Löschung der Daten ist über die von Klink zur Verfügung gestellte Verwaltungsoberfläche (Weboberfläche im Browser) von der Datengebenden Stelle selbst durchzuführen.
- Die Angaben der oben genannten Daten sind von der datengebenden Stelle freiwillig zu machen.
- Im Interesse beider Parteien soll die Datenbasis durch die Datengebende Stelle stets auf dem aktuellen Stand sein.
- Klink übernimmt keine Gewähr auf Richtigkeit und Vollständigkeit der Daten.
- Änderungen und Erweiterungen an der Datenbasis sind Klink jederzeit vorbehalten.

Anhang Verarbeitungszweck

Klink entwickelt eine mobile Applikation sowie eine Website – im Folgenden Applikation – welche die Datenbasis für Endnutzer:innen zugänglich macht. Die Applikation dient der Suche von Lokalitäten, die von Endnutzer:innen aufgesucht werden können, ähnlich einem Branchenbuch. Es sollen primär Lokalitäten mit Bewirtung in der Applikation von Klink gelistet werden. Darunter fallen Lokalitäten wie beispielsweise Bars, Kneipen, Restaurants, Diskotheken, Kinos und ähnliche weitere. Den Endnutzer:innen sollen innerhalb der Applikation alle relevanten Informationen angezeigt werden, die es ihnen erleichtern, die zu ihnen passendste Lokalität zu finden. Die von der Datengebenden Stelle zur Verfügung gestellten Daten können für diese Zwecke von Klink transformiert, angereichert und verändert werden.

Des Weiteren behält sich Klink das Recht vor, die von der Datengebenden Stelle zur Verfügung gestellten Daten im Rahmen einer statistischen Auswertung zu pseudonymisieren und mit weiteren Daten anzureichern. Diese Auswertungen dürfen an Kunden ausgehändigt werden.

Anhang Löschestätigung

Hiermit besttigt die

Könighaus, Schmelter, Biehs & Moes Klink GbR,

nachfolgend – Klink –,

dass sämtliche Daten (Datenbasis und Derivate), die Klink im Rahmen des Datennutzungsvertrages mit der Lokalität

zur Verfügung gestellt wurden, entsprechend dem Datennutzungsvertrag zum Ende der Vertragslaufzeit von allen Rechnern, Servern und Datenträgern sicher und vollständig gelöscht wurden.

Ort, Datum

Unterschrift Klink