Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

[DRK-Gliederung]
[Str.], [PLZ], [Ort]

nachstehend **„Verantwortlicher“**

und

DRK-Service GmbH
Berliner Straße 83
13189 Berlin

nachstehend **“Auftragsverarbeiter“**

Präambel

Die folgende Auftragsverarbeitung-Vereinbarung (AVV) erläutert, wie die DRK-Service GmbH in

- Dienstleistungsdatenbank (DLDB) und
- Benutzerverwaltung (BVw)

die Mitarbeiter-, Interessenten- und Kundendaten als personenbezogene Daten der DRK-Gliederungen und GmbHs vearbeitet.

DLDB und BVw enthalten die notwendigen Mitarbeiterdaten, damit

- die Datenbankzugänge zur Wissensbörse, DLDB, BVw, usw. und das Single-Sign on (ein Login für viele Datenbanken) möglich sind,
- die Rollen- und Zugriffsrechte, die von jeder DRK-Gliederung je Mitarbeiter selbst vergeben werden, gelten,
- die Ansprechpartnerdaten in der Rotkreuz-App erscheinen,
- die bundesweite Angebots-, Kurstermin- oder Kleidercontainersuche funktioniert,
- die Beratungszentren Kundenwunsch-Tickets zielgenau an Ihre Mitarbeiter senden können und Ihre Mitarbeiter die Tickets öffnen können,
- die Ticketübersicht über die DLDB in der Kundendatenbank aufgerufen werden kann,
- Daten aus Onlineformularen per gesicherter Datenübertragung an den zuständigen Sachbearbeiter zugestellt werden können,
- die Marketingforen auf DRK-intern.de besucht werden können und
- auch der Zugang zum Styleguide (Erscheinungsbild) und Mitgliederbrief so erfolgen kann, wie Sie dies in der BVw einstellen.

Ferner kann jede DRK-Gliederung über die DLDB auf die Workflowübersicht aller Tickets mit Kundenwünschen zugreifen, damit auch bei Abwesenheit des Sachbearbeiters der Kundenwunsch bearbeitet werden kann. Diese enthalten Interessenten- und Kundendaten.

Diese Mitarbeiter-, Interessenten- und Kundendaten sind nach DSGVO personenbezogene Daten, die AVV regelt ihre Speicherung und Bearbeitung in BVw und DLDB.

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „**DSGVO**“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als „**Vereinbarung**“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Nutzungsverhältnis (nachfolgend auch als „**Hauptvertrag**“ bezeichnet). Sofern Bezug auf die Regelungen des Bundesdatenschutzgesetzes (nachfolgend „**BDSG**“) genommen wird, so ist damit das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 in der zum Zeitpunkt ab dem 25. Mai 2018 geltenden Fassung gemeint. Wird Bezug auf die Regelungen des Bundesdatenschutzgesetzes-alt („**BDSG-alt**“) genommen, so ist damit das Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66) gemeint.

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

§ 1 Anwendungsbereich und Begriffsbestimmungen

(1) Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragsverarbeiter auf Grundlage des Hauptvertrages gegenüber dem Verantwortlichen erbringt.

(2) Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ von Daten benutzt wird, ist darunter allgemein die Verwendung von personenbezogenen Daten zu verstehen. Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Auf die weiteren Begriffsbestimmungen in Art. 4 DSGVO wird verwiesen.

§ 2 Gegenstand und Dauer der Datenverarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

(2) Gegenstand des Auftrags ist die Bereitstellung von Datenbanken,
- die den Zugang und die Zugriffsrechte zu anderen Datenbanken regeln,
- die die Angebote der DRK-Gliederungen und ihrer Ansprechpartner enthalten, sowie

- einer Software-Lösung zum Zwecke des Kunden-, Mitglieds-, Spender-, Kursteilnehmer-, Aktiven/Helfer- und Interessentenmanagementes

durch den Auftragsverarbeiter gegenüber dem Verantwortlichen im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs, gemäß dem Hauptvertrag.

(3) Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

§ 3 Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dieser umfasst den technischen Betrieb und das Hosting der Datenbanken BVw („DRK Benutzerverwaltung“), DLDB („Dienstleistungsdatenbank“) und KDB („Kundendatenbank“) durch den Auftragsverarbeiter. Der Auftragsverarbeiter speichert Mitarbeiterdaten und Anfragen und Daten von Kunden, Mitgliedern, Spendern, Kursteilnehmern, Aktiven/Helfern, Interessenten und Mitarbeitern zum Abruf und zur weiteren Nutzung durch den Verantwortlichen.

§ 4 Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit den personenbezogenen Daten im Rahmen dieser Vereinbarung betroffenen Personen umfasst:

- Mitarbeiter des Verantwortlichen,
- Interessenten für ein Angebot des Verantwortlichen,
- Interessenten für eine Fördermitgliedschaft oder ehrenamtliche Mitarbeit beim Verantwortlichern und
- Kursinteressenten des Verantwortlichen

§ 5 Art der personenbezogenen Daten

Von der Auftragsverarbeitung sind folgende Datenarten betroffen:

a) <u>Mitarbeiterdaten</u>

- Name, Vorname
- Foto des Mitarbeiters
- Gliederung, Gliederungs-ID
- dienstliche Aufgabe(n)
- dienstliche Kontaktdaten
- Zugriffsberechtigungen
- Angaben zur Bearbeitung von Anfragen (Zeitstempel)
- Logfiles über die Benutzung der Datenbanken

b) <u>Kunden- und Interessentendaten</u>

- Name, Vorname
- Kontaktdaten
- Geburtsdatum
- Familienstand

- DRK Mitgliedsnummer
- Beruf, Arbeitgeber, Position
- Bankverbindung
- Zahlungsdaten
- Art der Anfrage zur nachgefragten Dienstleistung,
- Art der gewünschten Kontaktaufnahme
- Status der Bearbeitung einer Anfrage
- Daten zu Angehörigen und Bezugspersonen

§ 6 Rechte und Pflichten des Verantwortlichen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr.7 DSGVO.

(2) Der Verantwortliche ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind auf Verlangen des Verantwortlichen unverzüglich vom Auftragsverarbeiter schriftlich oder in Textform (z.B. per E-Mail) zu bestätigen.

(3) Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.

(4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter festgestellt werden.

§ 7 Pflichten des Auftragsverarbeiters

(1) <u>Datenverarbeitung</u>

Der Auftragsverarbeiter wird personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Hauptvertrages sowie nach den Weisungen des Verantwortlichen zu verarbeiten.

(2) <u>Betroffenenrechte</u>

a. Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte der Auftragsverarbeiter die in § 5 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, wird der Auftragsverarbeiter dem Verantwortlichen den betreffenden Datensatz innerhalb einer angemessen gesetzten Frist, im

Übrigen innerhalb von sieben Arbeitstagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

b. Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die in § 5 dieser Vereinbarung genannten personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.

c. Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der in § 5 dieser Vereinbarung genannten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich nach Erhalt an den Verantwortlichen weiterleiten.

(3) Kontrollpflichten

a. Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.

b. Der Auftragsverarbeiter wird sein Unternehmen und seine Betriebsabläufe so gestalten, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

c. Der Auftragsverarbeiter bestätigt, dass er gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht. Datenschutzbeauftragter des Auftragsverarbeiters ist derzeit:

Felix Bonstein
ISiCO Datenschutz GmbH
Am Hamburger Bahnhof 4
10557 Berlin

(4) Informationspflichten

a. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

b. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützen.

(5) Ort der Datenverarbeitung

Die Verarbeitung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(6) Löschung der personenbezogenen Daten nach Auftragsbeendigung

Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern der Löschung dieser Daten keine gesetzlichen Aufbewahrungspflichten des Auftragsverarbeiters entgegenstehen. Die datenschutzgerechte Löschung ist zu dokumentieren und gegenüber dem Verantwortlichen auf Anforderung zu bestätigen.

Der Verantwortliche hat die Möglichkeit, Interessentendaten jederzeit selbst zu löschen. Für den Fall, dass eine solche Löschung nicht nach spätestens 12 Monaten erfolgt, erteilt der Verantwortliche dem Auftragsverarbeiter hiermit die Weisung, Interessentendaten spätestens nach zwölf Monate zu löschen.

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Verantwortliche und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.

(2) Der Auftragsverarbeiter wird den Verantwortlichen über die Durchführung von Kontrollmaßnahmen der Aufsichtsbehörde informieren, soweit die Maßnahmen oder Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

§ 9 Unterauftragsverhältnisse

(1) Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in § 9 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.

(2) Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der **Anlage 2** benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

(3) Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Änderung Einspruch erheben.

(4) Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragsverarbeiter zu erheben. Im Fall des Einspruchs kann der Auftragsverarbeiter nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragsverarbeiter nicht zumutbar ist – etwa aufgrund von damit verbundenen uverhältnismäßigen Aufwendungen für den Auftragsverarbeiter – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können der Verantwortliche und der Auftragsverarbeiter diese Vereinbarung sowie den Hauptvertrag mit einer Frist von einem Monat zum Monatsende kündigen.

(5) Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Der Auftragsverarbeiter ist gegenüber dem Verantwortlichen für sämtliche Handlungen und Unterlassungen der von ihm eingesetzten weiteren Auftragsverarbeiter verantwortlich.

§ 10 Vertraulichkeit

(1) Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet.

(3) Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die Vornahme der Verpflichtungen wird der Auftragsverarbeiter dem Verantwortlichen auf Nachfrage nachweisen.

(4) Sofern der Verantwortliche anderweitigen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

§ 11 Technische und organisatorische Maßnahmen

(1) Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt, dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht wesentlich herabgesetzt wird.

(2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art 32 i.V.m Art. 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

§ 12 Haftung/ Freistellung

(1) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.

(2) Der Verantwortliche stellt den Auftragsverarbeiter von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch den Verantwortlichen gegen den Auftragsverarbeiter geltend gemacht werden.

§ 13 Sonstiges

(1) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sich auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.

(3) Diese Vereinbarung unterliegt deutschem Recht.

(4) Vor dem 25. Mai 2018 gilt dieser Vertrag als Vertrag über die Auftragsdatenverarbeitung im Sinne des § 11 BDSG-alt. Die Regelungen des BDSG-alt gelten bis zum 25. Mai 2018 entsprechend.

(5) Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.

_____ Berlin, 31.01.2019

Ort, Datum

_____

Unterschrift (Verantwortlicher) **DRK-Service GmbH**

Anlagenverzeichnis

Anlage 1 Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Anlage 2 Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Anlage 1

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Der Auftragsverarbeiter sichert die Einhaltung der nachfolgend aufgeführten technischen und organisatorischen Maßnahmen als Mindestschutzniveau zu:

A) Maßnahmen zur Pseudonymisierung

Das CRM-System ist eine Datenbank, die für alle Nutzer Klarheit schaffen muss, um welchen Kunden es sich handelt und welche Aufträge für diesen ausgeführt werden sollen. Entsprechend dieser Zwecksetzung wird auf Maßnahmen zur Pseudonymisierung verzichtet.

B) Maßnahmen zur Verschlüsselung

Verschlüsselt werden alle persönlichen Passwörter für den Zugang den Datenbanken mit Ausnahme des Firmenportals.

Alle Datenübertragungen finden per SSL-Verschlüsselung mit HHTS auf der Grundlage eines SHA-256 mit RSA-Verschlüsselung statt. Zielsetzung dieser Technik ist die Verhinderung eines Man-in-the Middle-Datenabgriffs.

Weil die Daten für bestimmte Funktionen durchsuchbar sein müssen, ist eine direkte Verschlüsselung der Datenbanken nicht zu empfehlen. Dabei würde eine verschlüsselte Datenspeicherung in einer Datenbank z.B. eine Volltextsuche unmöglich machen. Die Übertragung der Daten zwischen den Hosts (Servern & Backupsystem) erfolgt ausschließlich verschlüsselt.

C) Maßnahmen zur Sicherung der Vertraulichkeit

1) Zutrittskontrolle

<u>Bereich Serverräume:</u>

Die Server werden bei der Firma Hetzner Online AG gehostet und von der Firma Bnet GmbH gemanagt. Die Server stehen im Datacenterpark Falkenstein, genau im RZ14.

- Personalisierte Zutrittskontrollsysteme mit Zutrittsberechtigung nur für autorisierte Mitarbeiter,
- Dienstanweisungen zur Handhabung von Zutrittskontrollen,
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude,
- Zugang zu Serverräumen ist nicht möglich, bzw. nur in Ausnahmefällen durch autorisierten Vertragspartner nach Terminvereinbarung, die sich vor Ort ausweisen können. Vertretungsberechtigte benötigen eine schriftliche Bestätigung des Vertragspartners.
- Videoüberwachung
- Der Zugang zu den Serverräumen ist nur in Begleitung eines Mitarbeiters möglich, ausgenommen des abgegrenzten Colocation-Bereiches.
- 24/7-Besetzung des Rechenzentrums.

Bereich Büroräume (DDM-Finckensteinallee 40) :

- Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen.
- Zutritt zu den Betriebsräumen haben nur Mitarbeiter mit personalisiertem Funktransponder
- Gäste haben nur in Begleitung von Mitarbeitern Zutritt.

2) Zugangskontrolle

Bereich Serverräume:

- Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar
- Clientsysteme nur nach passwortgeschützter Netzwerk-Authentifizierung nutzbar
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine nicht personalisierten Sammelkonten
- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passworten
- Richtlinie zur Erneuerung der Passwörter in bestimmten Zeitintervallen.

Bereich Büroräume (DDM-Finckensteinallee 40):

- Pro Benutzer wird eine individuelle Benutzerkennung vergeben.
- Passworte werden ausschließlich vom Benutzer erstellt und können vom Systemadministrator nicht eingesehen werden.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine nicht personalisierten Sammelkonten

3) Zugriffskontrolle

Zugang - Serverlandschaft:

- Der direkte Datenbankzugang ist nur mit einem „private public key-Verfahren“ mit SSH-Schlüssel möglich.
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren
- Revisionssicheres, verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Projektleitung / Abteilungsleitung / Geschäftsleitung / Geschäftsführung)
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)

Zugang - Datenbankapplikationen:

- Individuelle Zuweisung von Rechten pro Benutzer (Abgestufte Zugriffsberechtigung).
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung

- Jeder Systemzugriff wird protokolliert.
- Zugang durch https-gesicherte Weblogin-Seite

4) Trennungskontrolle

Bereich Büroräume (DDM-Finckensteinallee 40):

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden logisch getrennt voneinander gespeichert

Bereich Rechenzentrum:

- Daten verschiedener Gliederungen werden logisch getrennt voneinander gespeichert.
- Die Daten des Verantwortlichen werden physikalisch getrennt von Daten anderer Kunden gespeichert (dedizierte Server)

D) Maßnahmen zur Sicherung der Integrität

1) Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Livesystem mit Entwicklungen auf Developersystem und Stagingsystem,
- Debian Paketverwaltungssystem mit Linuxdistribution mit den Status:
    - Testing,
    - Stable,
    - Langzeitsupport
- Checklisten je KDB, FMV, KTV zur Funktionsprüfung,
- Logging: Änderungen werden mitgeschrieben per Syslog, ferner Logs innerhalb der Anwendungen zu Datenänderungen,
- Transporte von Datenträgern sind nicht erforderlich oder vorgesehen,
- der Austausch und die Vernichtung von ausgedienten Festplatten geschieht innerhalb des Rechenzentrums.

2) Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

Beschreibung der Übertragungskontrolle:

- Alle Datenübertragungen finden per SSL-Verschlüsselung mit HTTPS auf der Grundlage eines SHA-256 mit RSA-Verschlüsselung statt.
- Datentransfer ansonsten findet nicht statt.

3) Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

- Datenverschlüsselung
- Leitungsverschlüsselung

4) Eingabekontrolle

Bereich Büroräume (DDM-Finckensteinallee 40):

- Jede Dateneingabe wird protokolliert.

Bereich Rechenzentrum:

- Registrierung der Benutzer und Uhrzeit der jeweiligen Änderung im Teilnehmerverwaltungssystem

5) Auftragskontrolle

Bereich Büroräume (DDM-Finckensteinallee 40):

- Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften des BDSG sicherzustellen.
- Es ist ein betrieblicher Datenschutzbeauftragter bestellt, der die relevanten betrieblichen Prozesse überwacht.

Bereich Rechenzentrum:

- Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Verantwortlichen
- Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Verantwortlichen.
- Der Dienstleister hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse

E) Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

1) Verfügbarkeitskontrolle

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Einsatz unterbrechungsfreier Stromversorgung

- Alle Punkte gelten für das Rechenzentrum als auch für die Büroräume DDM-Fincken-stein-allee

2) Rasche Wiederherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Wiederherstellbarkeit:

Backup Web:
Sicherung nach GVS-Prinzip kreuzweise zwischen den Servern und zum BamseNet-Backupserver.

Backup Datenbank:
Lokales Backup (SQL-Dump) durch backupninja auf jedem Server im 4h-Rhythmus (1/5/9/13/17/21 Uhr). Vorgehalten wird hier jeweils nur die letzte Version. Diese wird mit der GVS-Sicherung archiviert.

Ansprechpartner: Firma Bnet, Herr Mittmann, Herr Körner, Herr Kummer, Herr Reinhardt

Verwaltungssoftware: Die Verwaltung erfolgt via Konsole.
Raid: vorhanden (Raid-Level 1)

Backup Server: kreuzweise Backups zwischen den DRK-Rootservern bei Hetzner und auf dedizierten Backupserver von BamseNet (bkup02.bamsenet.de).

Kreuzweise Backups:

- drk03 sichert drk01, drk04, inxmail
- drk04 sichert drk01, drk02, drk03
- bkup02 sichert drk01-04, inxmail

Backup Bereich DDM:
Sicherung nach dem GVS-Prinzip

Ansprechpartner : Herr Tzschach, Herr Ungeheuer, Herr Aydemir
Verwaltungssoftware: Windows Server Manager
Raid: vorhanden (Raid-Level 5)

<u>Szenario der Sicherung Rechenzentrum:</u>

GVS-Sicherung per rsync/rsnapshot via SSH (verschlüsselt zwischen den Servern):

- stündlich: 4h-Rhythmus, 6 vorgehaltene Versionen (letzte 24h)
- täglich: 1x täglich, das Älteste von hourly, 7 vorgehaltene Versionen (letzte Woche)
- wöchentlich: 1x wöchentlich, das Älteste von daily, 4 vorgehaltene Versionen (letzter Monat)
- monatlich: am 1. des Monats, 3 vorgehaltene Versionen (letztes Quartal)

RAID Level1 System

Das in den Root Servern vorhandene RAID Level1-System verfügt über zwei im Server eingebaute Festplatten. Beide werden gleichzeitig mit Daten beschrieben und verfügen somit immer über die identischen Daten (sog. Spiegelung). Diese Lösung bietet dadurch volle Redundanz, erhöht die Ausfallsicherheit und sorgt für permanente Verfügbarkeit der Daten: fällt eine Festplatte aus, arbeitet die andere weiter - die Daten sind weiterhin abrufbar. Erst der Ausfall beider Platten führt zum Totalverlust der Daten.

Zeitabstand zwischen den Absicherungen

Für die Server des CRM-Systems werden tägliche Absicherungen, sowohl von den Webdaten als auch von den Datenbanken durchgeführt (s. Punkt 3.1).

Anzahl der aufbewahrten Absicherungen

- Betriebszeitraum letzte 24 Stunden: 6 Sicherungen und
- Betriebszeitraum > 24h bis 7. Tag: 6 Sicherungen und
- Betriebszeitraum > 7. Tag bis 4.Woche: 3 Sicherungen und
- 4. Woche bis 3. Monat: 3 Sicherungen

Aufbewahrung der Datensicherungen

Der physikalische Zugriff auf die Server ist nicht möglich, ausgenommen wenn Zutritt zum Hetzner- Rechenzentrum besteht. Zutritt zum Rechenzentrum ist nur Mitarbeitern der Firma Hetzner gestattet. Es liegt eine schriftliche Erklärung über die Verpflichtung auf das Datengeheimnis (§ 5 BDSG) der Mitarbeiter bei der Hetzner Online AG durch die Datenschutzbeauftragte der Hetzner Online AG vor. Generell sind nur die notwendigen Ports für den Betrieb von Web- und Maildiensten von außen zugänglich. Das zusätzliche Backupsystem der Firma Bnet GmbH steht in einem gesonderten Rechenzentrum (RZ13) am Standort Falkenstein.

Zeitfenster - Betriebsbeeinträchtigungen

Es entstehen keine Betriebsbeeinträchtigungen durch die Sicherungen.

<u>Szenario der Sicherung Büroräume DDM:</u>

GVS-Sicherung per Software von ArcServe

- täglich: 1x täglich (Mo.- Do.)
- wöchentlich: 1x wöchentlich (Freitag), 3 vorgehaltene Versionen
- monatlich: am Ende des Monats, 2 vorgehaltene Versionen (letzter Monat)

- **RAID Level 5 System**

In RAID 5-Stripesets werden Daten und Kontrollinformationen (Parity) über vier Festplatten verteilt. Der Controller ist für die Berechnung der Kontrollinformationen zuständig, die bei jedem Schreibvorgang erzeugt und beim Lesen überprüft werden. Der dabei entstehende zusätzliche Index wird ebenfalls über alle Laufwerke verteilt. Die Parität wird durch eine Exklusiv-oder-Verknüpfung realisiert. Eine Festplatte innerhalb des RAIDs darf vollständig ausfallen, ohne dass Daten verloren gehen. Das System kann weiterhin auf das Array und die Daten der fehlerhaften Platte zugreifen, weil ihre Daten aufgrund der Exklusiv-oder-Operation unter Zuhilfenahme der Parität aus den verbliebenen Platten errechnet werden können.

Ein RAID 5 System stellt den besten Kompromiss zwischen Datenschutz, Verfügbarkeit und

Leistung dar.

- **Anzahl der aufbewahrten Absicherungen**
  - Betriebszeitraum: 1 bis 4. Wochentag: 4 Sicherungen und
  - Betriebszeitraum: 5. Wochentag (1-3 Woche): 3 Sicherungen und
  - Betriebszeitraum: 5. Wochentag (4. Woche): 2 Sicherungen

- **Aufbewahrung der Datensicherungen**

Aufgrund der räumlichen Gegebenheiten erfolgt die Aufbewahrung der Sicherungen in einem verschlossenen Bereich.

- **Zeitfenster - Betriebsbeeinträchtigungen**

Es entstehen keine Betriebsbeeinträchtigungen durch die Sicherungen.

Vollständigkeit und Integrität der Datensicherungen

- Rechenzentrum

Die Vollständigkeitskontrolle der Datensicherungen, wird über die Kontrolle des Datenzuwachses auf den Systemen (im Monitoringsystem Muning) und das Logging gewährleistet. Zudem informieren die Jobs automatisch bei Störungen die Administratoren der BamseNet GmbH. Weiterhin werden alle Systeme regelmäßig einer manuellen Kontrolle unterzogen. Der gesamte Betrieb der Server (hiermit auch der Sicherungsverlauf) wird permanent mit den Softwarepacketen Munun, Nagios und dem Core-Monitoring des RZ überwacht.

- Büroräume DDM-Finckensteinallee

Die Vollständigkeitskontrolle der Datensicherungen, wird über die Kontrolle des Datenzuwachses auf den Systemen (Arcserve) und das Logging gewährleistet. Zudem informieren die Jobs automatisch bei Störungen den Administrator. Weiterhin werden alle Systeme regelmäßig einer manuellen Kontrolle unterzogen. Der gesamte Betrieb der Server (hiermit auch der Sicherungsverlauf) wird regelmäßig überwacht.

Datenverlust - Wiederherstellung der Daten - Ersatzsystem beim Ausfall

- Rechenzentrum

Der maximale Datenverlust liegt hier im Bereich von 4h, wenn der Fehler innerhalb von 24h bemerkt wird, danach entsprechend grobmaschiger. Der Datenverlust bei Feststellung eines Fehlers (z.B. versehentlichen Löschens von Dateien) zu einem späteren Zeitpunkt errechnet sich aus dem o.g. Sicherungsregimes. Der Ausfall einer einzelnen Festplatte in einem Server führt in Regel zu keinem Datenverlust, da die Platten im gespiegelten Verbund (RAID 1) laufen.

- Büroräume DDM-Finckensteinallee

Der maximale Datenverlust liegt hier im Bereich von 24h, wenn der Fehler innerhalb von 24h bemerkt wird, danach entsprechend grobmaschiger. Der Datenverlust bei Feststellung eines Fehlers (z.B. versehentlichen Löschens von Dateien) zu einem späteren Zeitpunkt errechnet sich aus dem o.g. Sicherungsregimes. Der Ausfall einer einzelnen Festplatte in einem Server

führt in der Regel zu keinem Datenverlust, da die Festplatten in einem Verbund (RAID 5) laufen.

Rücksicherungstest

Es sind in der Vergangenheit keine systematischen Rücksicherungstests durchgeführt worden. Bei gelegentlichen Änderungen bzw. Anpassungen von Scripten wurden Rücksicherungstests zur Kontrolle der Funktionalität durchgeführt.

3) Zuverlässigkeit

- Rechenzentrum

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Der Auftragsverarbeiter beauftragt Fa. Bnet GmhH als technischen Dienstleister (TDL) mit dem laufenden Betrieb der Datenbanken und eine technische Störungshotline mit täglicher Erreichbarkeit zwischen 7:00 und 22:00 Uhr auch an Sonn- und Feiertagen mit folgenden Aufgaben

(a) Gewährleistung des laufenden Betriebs der Datenbanken und der dazu erforderlichen Webserver; Spiegelung der Daten auf einem weiteren Server und Bereitstellung eines Ersatzsystems im Störungsfalle;
(b) Systempflege und regelmäßige Wartung der Datenbanksoftware und der Websever, auf denen die Datenbanken gehostet werden;
(c) Einspielen von Updates und Sicherheitspatches für die Webserver sowie Einspielung und Einrichtung von aktualisierter Webserversoftware;
(d) eingehende technische Prüfung und anschließende Installation von Updates und anderen Änderungen der Datenbanksoftware, die durch DRK oder einen beauftragten Dritten entwickelt wurden;
(e) Bereitstellung eines Test- und Entwicklungssystems für die Weiterentwicklung der Datenbanksoftware.

Für die Störungs-Hotline gilt folgender Workflow:

- Automatisches Monitoring mit E-Mail-Benachrichtigung, Check-MK-Verfahren im Einsatz mit Mailbenachrichtigung plus Messengerbenachrichtigung

- Notfallpläne mit Verantwortlichkeiten und IT-Notdienst 24/7
  wir haben Hotline mit 24/7 mit Kundenpriorisierung

- Büroräume DDM

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beauftragt als Administrator ist Herr Tzschach. Werktägliche Erreichbarkeit zwischen 8:00 und 18:00 Uhr mit folgenden Aufgaben:

(a) Gewährleistung des laufenden Betriebs und der dazu erforderlichen Server und IT-Perepherie; Bereitstellung eines Ersatzsystems im Störungsfalle;

(b) Systempflege und regelmäßige Wartung von Software und Serversystem
(c) Einspielen von Updates und Sicherheitspatches für die Server sowie Einspielung und Einrichtung von aktualisierter Backup- und Antivirensoftware

Für die Störungs-Hotline gilt folgender Workflow:

- Notfallpläne mit Verantwortlichkeiten und IT-Notdienst mit 24/7 Hotline mit 24/7 mit Kundenpriorisierung

Datenwiederherstellung

- Rechenzentrum
Für den Fall eines durch DRK-Gliederung selbstverursachten Verlustes von Daten wie z.B. Kunden-, Mitglieder-, Spender- oder Kursteilnehmerdaten stellt DRKS ein mandantenbasiertes zentrales Backup bereit. Bei Datenverlust kann DRK-Gliederung zwischen verschiedenen aktuellen Backups wählen (von einem Tag alt bis maximal vier Wochen). Es werden vier freitägliche Sicherungen aufgehoben. Eine gewünschte Neueinspielung muss kostenpflichtig gegenüber dem technischen Dienstleister beauftragt werden, der auch die Berechnung vornimmt. Die Auftragserteilung muss schriftlich erfolgen an die Störungshotline; Telefonnummer: 0351 89 66 36 66, Faxnummer: 0351 89 663 629 oder Email: Service@Bnet.de.

Einzeltests sind belegbar, finden nicht regelmäßig statt.

- Büroräume DDM
Für den Fall eines Verlustes von Daten wie z.B. Exchange-Mails, Bilddaten oder Dokumenten stellt die DRKS ein zentrales Backup bereit. Bei Datenverlust kann DDM-F40 zwischen verschiedenen aktuellen Backups wählen (von einem Tag alt bis maximal acht Wochen). Es werden 3 freitägliche Sicherungen aufgehoben. Telefonnummer: 030 868 778 323 oder Email: i.tzschach@drkservice.de.

Einzeltests sind belegbar, finden nicht regelmäßig statt.

F) Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

1) Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen:

Das Datenschutzmanagement umfasst das Verfahrensregister der DRKS, die Auftragsvereinbarung, das Sicherheitskonzept, einen im Jahr 2018 durchgeführten Penetrationstest und IT-Check der Fa. Tasco, verschiedene Organanweisungen und die Aktivitäten des Datenschutzbeauftragten.
Zertifizierung des Rechenzentrum - Hetzner Online ist nach DIN ISO/IEC 27001 zertifiziert Der international anerkannte Standard für Informationssicherheit bescheinigt der Hetzner Online GmbH, dass ein geeignetes Informationssicherheitsmanagementsystem, kurz ISMS, implementiert und adaptiert wurde. Das ISMS findet an den Standorten

Nürnberg und Falkenstein bei der Infrastruktur und dem Betrieb der gesamten Datacenterparks Anwendung und wurde durch die FOX Certification geprüft. Link zum Zertifikat oder als Wissensbörse-Dokument Nr 22 231.

Formalisierte Prozesse für **Datenschutzvorfälle**

- Klärung des Vorfalls und Tragweite
- Information der DRKS-Geschäftsführung,
- Je nach Schwere Information an die betroffenen DRK-Gliederungen und Datenschutzbeauftragten des betroffenen Landesverbands
- Meldung an Aufsichtsbehörde im Auftrag der DRKS-Geschäftsführung

- Service-Level-Agreements für die Durchführung von Kontrollen

2) Auftragskontrolle

- Der Auftragsverarbeiter macht detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Verantwortlichen.
- Der Auftragsverarbeiter macht detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Verantwortlichen.
- Der Auftragsverarbeiter hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.

Ergibt sich aus den Prüfungen Umsetzungsbedarf hinsichtlich der auftragsspezifischen vereinbarten Maßnahmen oder werden Änderungen der Maßnahmen aus anderen Gründen erforderlich, sind diese zunächst mit dem Verantwortlichern abzustimmen. Die zu ergreifenden Maßnahmen können sich insbesondere auch aus konkreten Weisungen im Einzelfall des Verantwortlichen ergeben.

Anlage 2

Unterauftragsverhältnisse gemäß § 9 der Vereinbarung zur Auftragsverarbeitung

Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

1. b.Net GmbH

Name/Firma:	b.Net GmbH
Funktion/Tätigkeit:	Hosting- und Wartungsdienstleistungen
Sitz [Stadt, Land]:	Hamburger Straße 19c, 01067 Dresden, Deutschland

2. Zwei-G Netzwerk

Name/Firma:	Zwei-G Netzwerk
Funktion/Tätigkeit:	Softwareprogrammier- und -wartungsdienstleistungen
Sitz [Stadt, Land]:	Großstückenweg 7b, 01445 Radebeul, Deutschland