Greenmark IT GmbH
Leinstr. 3, 31061 Alfeld (Leine)

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung zwischen der

Gerald Thomiszer
Markt 90
4363 Pabneukirchen
Kundennummer: K6539

[Auftraggeber]

und der

Greenmark IT GmbH
Leinstraße 3
D-31061 Alfeld (Leine)

[Auftragnehmer]

ggf.: Vertreter gemäß Art. 27 DSGVO:

§ 1 Gegenstand und Dauer des Auftrags

1.1 Der Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Der Auftragnehmer ist Domainprovider / Registrar für verschiedene Domainendungen und stellt über das Webinterface als auch über eine API-Schnittstelle Domain-Produkte zum Kauf zur Verfügung.

Der Auftragnehmer ist IT-Dienstleister für Hosting-Produkte (Webspace / vServer, Server) und stellt diese über das Webinterface zum Kauf zur Verfügung.

Der Auftragnehmer bietet SSL-Zertifikate an und stellt über ein Web-Interface die Produkte zum Kauf zur Verfügung.

1.2 Der Auftrag ist unbefristet erteilt und gilt solange, wie Leistungen durch den Auftraggeber bezogen werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 2 Konkretisierung des Auftragsinhalts

Einzelheiten zu Art und Zweck der vorgesehenen Verarbeitung oder Nutzung sind unter Buchstabe A. der Anlage 1 zu dieser Vereinbarung aufgeführt. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Das angemessene Schutzniveau

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften [Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO];
☐ wird hergestellt durch Standarddatenschutzklauseln [Art. 46 Abs. 2 litt. c und d DSGVO];
☐ wird hergestellt durch genehmigte Verhaltensregeln [Art 46 Abs. 2 lit. e i.V.m. 40 DSGVO];
☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus [Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO].
☐ wird hergestellt durch sonstige Maßnahmen: [Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DSGVO]
Die Art der personenbezogenen Daten sind unter Buchstabe B. der Anlage 1 aufgeführt.
Der Kreis der Betroffenen ist unter Buchstabe C. der Anlage 1 aufgeführt.

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

§ 3 Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 2].

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

5.1 Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
☑ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

5.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.3 Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

5.4 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5 Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

5.6 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

5.7 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzes-konforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

6.3 Der Auftraggeber erklärt sich mit dem Einsatz nachfolgend genannter weiterer Auftragsverarbeiter einverstanden: [siehe Anlage 4: Unter-Auftragsverarbeiter]

6.4 Der Auftragnehmer informiert den Auftraggeber, wenn er beabsichtigt, Auftragsverarbeiter zu wechseln oder neue hinzuzuziehen. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

6.5 Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

6.6 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.7 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.8 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6.9 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers [mind. Textform]. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Kontrollrechte des Auftraggebers

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
☑ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen [z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren];
☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit [z.B. nach BSI-Grundschutz).

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen, wenn es sich um mehr als eine eintägige Vor-Ort-Kontrolle pro Jahr handelt.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich [mind. Textform].

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9.3 Weisungsberechtigte Personen des Auftraggebers werden in Anlage 3 genannt.

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

§ 10 Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Kündigungsrecht

Der Verantwortliche kann diesen Vertrag jederzeit ohne Einhaltung von Kündigungsfristen kündigen, wenn

- der Auftragsverarbeiter gegen eine wesentliche Pflicht dieses Vertrages oder die Vorschriften der DSGVO verstößt,
- der Auftragsverarbeiter eine Weisung des Verantwortlichen missachtet,
- der Auftragsverarbeiter die Ausübung von Kontrollrechten des Verantwortlichen verweigert oder nicht nur unerheblich behindert oder
- der Auftragsverarbeiter den Zutritt des Verantwortlichen oder eines entsprechend Beauftragten zu den Betriebsräumen, in denen Daten auf Grund dieses Vertrages verarbeitet bzw. genutzt werden, vertragswidrig verweigert.
- der Auftragsverarbeiter keine hinreichenden Garantien für die Sicherheit der Verarbeitung mehr bietet.

§ 12 Haftung

12.1 Verantwortlicher und Auftragsverarbeiter haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die einer betroffenen Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Verhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine betroffene Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatzanspruch, so kann diese von der jeweils anderen Partei Freistellung verlangen, soweit dies ihren Anteil an der Verantwortung entspricht.

Die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen für schuldhafte Verletzungen dieses Vertrags regelt sich nach den gesetzlichen Bestimmungen.

12.2 Der Auftragsverarbeiter haftet für ein Verschulden seines Unterauftragsverarbeiters und seiner Unter-Unterauftragsverarbeiter wie für eigenes Verschulden.

12.3 Der Auftragsverarbeiter trägt die Beweislast dafür, dass der Schaden oder Verlust nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit Daten unter diesem Vertrag verarbeitet werden. Der Auftragsverarbeiter kommt seiner Beweispflicht nach, wenn er darlegen kann, dass er bei der Erhebung bzw. Verarbeitung der Daten die Regelungen dieses Vertrags beachtet hat und insbesondere die technischen und organisatorischen Sicherheitsmaßnahmen wie vereinbart umgesetzt hat.

§ 13 Salvatorische Klausel, Gerichtsstand

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

13.1 Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

13.2 Als Gerichtsstand wird Alfeld (Leine) vereinbart.

PABNEUKIRCHEN, den 09.11.2022

Gerald Thomiszer

Auftraggeber

Alfeld (Leine), den 09.11.2022

GREENMARK IT
Greenmark IT GmbH
Leinstraße 3
31061 Alfeld (Leine)
info@greenmark-it.de
www.greenmark-it.de
Tel.: 05181 / 855 37 - 0
Fax: 05181 / 855 37 - 29
HRB 204773
USt-ID: DE264727629

A. Gundelach

Auftragnehmer

Anlage:

Anlage 1 - Art der personenbezogenen Daten / Kreis der Betroffenen
Anlage 2 - Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO
Anlage 3 - Ansprechpartner
Anlage 4 - Unter-Auftragsverarbeiter

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

Anlage 1:

A. Zu § 2 Ergänzungen zu Art und Zweck der Datenverarbeitung
Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung sind:

Der Auftragnehmer bearbeitet Domain-Aufträge des Auftraggebers die über das Webinterface oder API-Schnittstelle aufgegeben werden, sowie der damit im Zusammenhang stehenden Leistungen wie z.B. FlexDNS, Handle-Verwaltung, TMCH etc.

Je nach Auftrags-Operation werden zusätzliche personenbezogene Daten wie z.B. Personalausweise, Handelsregisterauszüge zur vollständigen Auftragserfüllung (nach Registry-Bedingungen) benötigt.
Im Zuge der Leistungserbringung des Auftragnehmers als zentraler Domainprovider / Registrar im Bereich der Domain-Verwaltung, des Supports bzw. der Verarbeitung von Domain-Aufträgen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

Der Auftragnehmer stellt dem Auftraggeber Webhosting-Diensleistungen bzw. eines (oder mehrerer) dedizierten/dedizierter Server sowie der damit im Zusammenhang stehenden Leistungen wie z.B. E-Mail, etc. Im Rahmen dieses Vertrages hat der Auftraggeber – je nach Produkt und vereinbarten Leistungsumfang – unter Nutzung u.a. z.B. eines Webservers, FTP-Servers oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (zu speichern, zu verändern, zu übermitteln und zu löschen).

Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

Der Auftragnehmer prüft, bearbeitet und validiert Zertifikatsanträge des Auftragsgebers, die über das Webinterface aufgegeben werden. Des Weiteren unterstützt er bei der Validierung von Zertifikatsanträgen (SSL-Zertifikate OV und EV). Bei der Prüfung und Validierung werden ggf. Unternehmen mit z.B. Handelsregisteranträgen und Telefonbuch-Einträgen abgeglichen.

B. Zu § 2 Art der personenbezogenen Daten

☑ - Personenstammdaten
☑ - Kommunikationsdaten (z.B. Telefon, E-Mail)
☑ - Vertragsstammdaten (Vertragsbeziehung, Produkt-bzw. Vertragsinteresse)
☑ - Kundenhistorie
☑ - Vertragsabrechnungs- und Zahlungsdaten
☑ - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

C. Zu § 2 Kreis der Betroffenen

☑ - Kunden
☑ - Interessenten
☑ - Abonnenten
☑ - Beschäftigte
☑ - Lieferanten
☑ - Handelsvertreter
☑ - Ansprechpartner

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

Anlage 2:

Allgemeine technische und organisatorische Maßnahmen (TOMs)
Zum Schutz von personenbezogener Daten gemäß Art. 32 DSGVO

Dieses Dokument dient zur Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, vorläufig zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem Auftraggeber bei wesentlichen Änderungen und im Übrigen jährlich zur Durchführung der Auftragskontrolle vorzulegen.

Dokumentationen der nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen.

1. Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO: Pseudonymisierung)
Wie wird die Pseudonymisierung der Daten gewährleistet?

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

Regelungen für digitale Pseudonymisierung	• Data Masking • Hashing

2. Verschlüsselung (Art. 32 Abs. 1 lit. A DSGVO: Verschlüsselung)
Wie wird die Verschlüsselung gewährleistet?

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

Techniken zur Verschlüsselung	• Data Hashing • Nutzung von kryptografischen Tools • TLS/SSL-Transportverschlüsselung • E-Mailverschlüsselung (PGP)

3. Fähigkeit der Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO: Zutrittskontrolle)

Nur befugte Personen haben Zugang zu den DV-Anlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Festlegung befugter Personen	• Räume sind verschlossen und nur befugte Personen haben einen Schlüssel • Elektronisch und mechanische Sicherheitssysteme für Haupteingangstüren im Bürogebäude • Dokumentierte Schlüsselvergabe an Mitarbeiter
Regelung für Firmenfremde	• Betriebsfremde Personen haben keinen Zugang zu den DV-Anlagen

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

Sicherung außerhalb der Arbeitszeit	• Alle Räume mit DV-Anlagen sind verschlossen • Alarmanlage

4. Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO: Zugangskontrolle)

Nur befugte Personen können DV-Systeme nutzen.

Workstations und Notebooks	• Notebooks und Workstations sind verschlüsselt • Authentifizierung über Benutzername/Passwort • Interne EDV-Richtlinien für den Umgang mit DV-Systemen
Verpflichtung auf das Datengeheimnis	• Wird von jeden Mitarbeiter durch die Vertraulichkeitsverpflichtungserklärung vertraglich geregelt
Benutzerberechtigungen	• Werden durch den zuständigen Bereichsleiter bestimmt • Dokumentation und Verwaltung von Benutzerberechtigung
Einsatz von 2-Factor Authentifizierung	• Wo es möglich ist, wird eine 2-Factor Authentifizierung verwendet
Kundenauthentifizierung	• Kunden authentisieren sich zusätzlich mittels geheimer Informationen (Servicepasswort) beim telefonischen Kontakt zum Kundensupport
Vernichtung von Datenträgern	• Wird durch ein zertifiziertes Unternehmen durchgeführt • Die Vernichtung wird protokolliert
Remotezugriff	• Der administrative Remotezugriff auf die DV-Anlagen ist ausschließlich über ein VPN möglich oder/und durch Keybasierte SSH-Zugänge
IT-Sicherheit	• Einsatz diverser Antivirenlösungen • Einsatz von Hard- und Softwarefirewalls
DV-Software	• zusätzlicher Login für bestimmte sicherheitsrelevante Software
Passwörter	• zu vergebende Passwörter werden durch die schriftlich fixierte Passwortrichtlinie für Mitarbeiter gewährleistet • die Speicherung erfolgt in einer extra verschlüsselten Passwortverwaltungssoftware • Passwörter werden in regelmäßige Abständen erneuert
Regelungen für analoge Pseudonymisierung	• Maschinelle Vernichtung mit mindestens Sicherheitsstufe (DIN 32757-1) 3 bzw. Sicherheitsstufe (DIN 66399) P-3, T-2

5. Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO: Zugriffkontrolle)

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

Regelung der Zugriffskontrolle	• Rechtevergabe erfolgt durch den IT-Leiter • Least to know Prinzip bei der Vergabe von Berechtigung • IT prüft die aktuellen Berechtigungen regelmäßig auf Notwendigkeit
Auswertung von Protokollen	• IT prüft regelmäßig die Protokolle auf Verletzungen der Richtlinien

Kontakt
E-Mail: service@do.de
Website: my.do.de
Fon: +49 5181 8553720
Fax: +49 5181 8553728

Register
HRB 204773
Amtsgericht Hildesheim
UstID: DE264727629

Geschäftsführung
Ali Jasarov
Andreas Gundelach

Bankverbindung
Kontoinhaber: Greenmark IT GmbH
IBAN: DE15 4306 0967 1066 4783 00
BIC: GENODEM1GLS
Bank: GLS Gemeinschaftsbank eG

Zeitliche Begrenzungen	• Auto-Logout bei allen Systemen • Bildschirmsperre • Wo es möglich ist, Sperren nach ungültigen Anmeldeversuchen • Wo es möglich ist, Zeitverzögertes Antwortverhalten bei Fehlversuchen

6. Integrität (Art. 32 Abs. 1 lit. B DSGVO: Weitergabekontrolle)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Festlegung befugter Personen	• Durch die Vergabe entsprechender Rechte
4-Augen-Prinzip	• Entwicklung, Administration und Support arbeiten nach dem 4-Augen-Prinzip
Datenträger	• Mobile Datenträger werden in der Regel nicht verwendet, falls doch sind diese verschlüsselt. • Festplatten werden überwacht, verschlüsselt und durch verschließbare Festplatteneinschübe gesichert
Remotezugriff	• Der administrative Remotezugriff auf die DV-Anlagen ist ausschließlich über ein VPN möglich oder/und durch Keybasierte SSH-Zugänge
Auswahl der Auftragnehmer	• Auswahl erfolgt in der Regel durch die Geschäftsführung
Aufteilung der Rechte und Pflichten zw. Auftragnehmer und Auftraggeber	• Geschieht über einen AV-Vertrag nach Artikel 28 DSGVO

7. Integrität (Art. 32 Abs. 1 lit. B DSGVO: Eingabekontrolle)

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Verpflichtung auf das Datengeheimnis	• Wird von jeden Mitarbeiter durch die Vertraulichkeitsverpflichtungserklärung vertraglich geregelt
Protokollierung von Systemzugriffen	• Zugriffe auf personenbezogene Daten werden protokolliert

8. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. B DSGVO)

Es ist zu gewährleisten, dass Systeme und Dienste die Fähigkeit besitzen, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit in Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

Rechenzentrum	• Die Dienstleistungen werden mit Hilfe mehrerer Rechenzentrumsdienstleisters erbracht, welche nach ISO 27001 zertifiziert sind
Backup und Desaster Recovery	• Backupdaten werden physikalisch und örtlich getrennt aufbewahrt

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

Zusätzliche Maßnahmen	• Unterbrechungsfreie Stromversorgung (USV) • Spiegelung von Festplatten
Langzeitarchivierung	• Geeignete Räumlichkeiten zur Archivierung

9. Zweckbindungskontrolle (Art. 28 Abs. 3 S. 2 b) DSGVO)

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Mandantentrennung	• Logische Mandantentrennung über die Software
Funktionstrennung	• Daten für unterschiedliche Zwecke werden durch virtualisierte oder hardwareseitige Mechanismen getrennt

10. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. D DSGVO; Art. 25 Abs. 1 DSGVO)

Verpflichtung auf das Datengeheimnis	• Wird von jeden Mitarbeiter durch die Vertraulichkeitsverpflichtungserklärung vertraglich geregelt
Protokollierung von Systemzugriffen	• Zugriffe auf personenbezogene Daten werden protokolliert
Rechenzentrum	• Die Dienstleistungen werden mit Hilfe mehrerer Rechenzentrumsdienstleisters erbracht, welche nach ISO 27001 zertifiziert sind
Backup und Desaster Recovery	• Backupdaten werden physikalisch und örtlich getrennt aufbewahrt
Mandantentrennung	• Logische Mandantentrennung über die Software
Funktionstrennung	• Daten für unterschiedliche Zwecke werden durch virtualisierte oder hardwareseitige Mechanismen getrennt
Datenschutzfreundliche Voreinstellungen	• Alle zur Datenverarbeitung genutzten Systeme werden in der Regel so datenschutzfreundlich wie möglich benutzt und konfiguriert • Eine Pseudonymisierung wird so früh wie möglich vorgenommen
Regelmäßige Überprüfung	• Interne Programmierungsrichtlinien geben Privacy by Default und Privacy by Design verpflichtend vor

Kontakt
E-Mail: service@do.de
Website: my.do.de
Fon: +49 5181 8553720
Fax: +49 5181 8553728

Register
HRB 204773
Amtsgericht Hildesheim
UstID: DE264727629

Geschäftsführung
Ali Jasarov
Andreas Gundelach

Bankverbindung
Kontoinhaber: Greenmark IT GmbH
IBAN: DE15 4306 0967 1066 4783 00
BIC: GENODEM1GLS
Bank: GLS Gemeinschaftsbank eG

Anlage 3:

Ansprechpartner

Weisungsberechtigte Person(en) des Auftraggebers:

Name: Gerald Thomiszer
E-Mail: admin@ff-pabneukirchen.at
Telefon: +436649279337

Datenschutzbeauftragter des Auftraggebers:

Name:
E-Mail:
Telefon:

Weisungsempfänger des Auftragnehmers:

Name: Malte Glöckner
E-Mail: m.gloeckner@greenmark-it.de
Telefon: +49 5181 8553722

Datenschutzbeauftragter des Auftragnehmers:

Name: PSW GROUP GmbH & Co. KG / Frau Ludwig
E-Mail: datenschutz@greenmark-it.de

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG

Anlage 4:

Unter-Auftragsverarbeiter

Folgende Unter-Auftragsverarbeiter werden aktuell eingesetzt:

- keine

Kontakt	Register	Geschäftsführung	Bankverbindung
E-Mail: service@do.de Website: my.do.de Fon: +49 5181 8553720 Fax: +49 5181 8553728	HRB 204773 Amtsgericht Hildesheim UstID: DE264727629	Ali Jasarov Andreas Gundelach	Kontoinhaber: Greenmark IT GmbH IBAN: DE15 4306 0967 1066 4783 00 BIC: GENODEM1GLS Bank: GLS Gemeinschaftsbank eG