Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Zwischen

_____

_____

_____

- Verantwortlicher - nachfolgend Auftraggeber genannt -

und

Bayerwald Media GmbH
Kirchplatz 10
93482 Pemfling

- Auftragsverarbeiter - nachfolgend Auftragnehmer genannt -
[ggf.: Vertreter gemäß Art. 27 DS-GVO:]

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

Bezieht sich auf alle bestehenden Rechtsgeschäfte (im Folgenden Leistungsvereinbarung) in deren Rahmen es zur Auftragsverarbeitung personenbezogenen Daten kommt.

1.2. Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von

_____ Monaten zum _____

gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der **Anlage 2**.

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. DS-GVO erfüllt sind.

Das angemessene Schutzniveau in _____

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

☐ wird hergestellt durch sonstige Maßnahmen: _____
(Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO)

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 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [**Einzelheiten in Anlage 1**].

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.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

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, ist Löschkonzept, Recht auf Vergessen werden, Berichtigung, Daten Portabilität 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 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Gerald Lill, Projekt 29 GmbH & Co. KG, Ostengasse 14, 93047 Regensburg bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

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

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

e) 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.

f) 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.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

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 gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu. Auf Verlangen des Auftraggebers hat der Auftragnehmer Einsicht in die bestehenden Vereinbarungen mit den Unterauftragnehmern zu gewähren.

Erfolgt eine Verarbeitung im Auftrag, so arbeitet der Auftragnehmer nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Der Auftraggeber kann jederzeit einem Einsatz von Subunternehmern gegenüber dem Auftragnehmer widersprechen. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

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

6.4. 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.

6.5. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
@ info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

7. Kontrollrechte des Auftraggebers

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 DS-GVO 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
a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
c) Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
d) 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.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO 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 nicht 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 in Schriftform.

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.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

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. Unterschrift „Auftraggeber“ „Auftragnehmer“

	Geschäftsführer, Stefan Wistuba
(Titel, Name, Unterschrift)	(Titel, Name, Unterschrift)
	Pemfling, den
(Ort, Datum)	(Ort, Datum)

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

Anlage 1 [TOMs]
Technische und organisatorische Maßnahmen

IMPRESSUM

Urheber:	Bayerwald Media GmbH
Titel:	Technische und organisatorische Maßnahmen
Version:	0.3
Vertraulichkeitsstufe:	Öffentlich
Gültig ab:	01.07.2020
Archivierungspflicht:	JA
Aufbewahrungsfrist:	6 Jahre
Archivierungsort:	Digital, Intranet

ÄNDERUNGSHISTORIE

Datum	Version	Beschreibung	Autor
05.04.2018	0.1	Initiale Erstellung des Dokuments	Stefan Wistuba
09.06.2018	0.2	Inhaltliche Änderungen	Stefan Wistuba
28.05.2020	0.3	Neuerstellung, verständlicher, ergänzt um die aktuellen Maßnahmen in Richtung mehr Sicherheit	Stefan Wistuba
29.05.2020	0.3	Prüfung der Richtigkeit der Inhalte	Nico Rank
04.06.2020	0.3	Prüfung der DSGVO Konformität	Gerald Lill
01.07.2020	0.3	Freigabe	Stefan Wistuba

HINWEIS

Es wird darauf hingewiesen, dass die ggf. im Dokument verwendeten Begrifflichkeiten nicht als diskriminierend im Sinne des Allgemeinen Gleichbehandlungsgesetzes zu verstehen sind. Bezeichnungen und Begriffe werden einheitlich geschlechtsneutral entsprechend der Funktion oder Tätigkeit verwendet; diese Funktions- und/oder Tätigkeitsbezeichnungen haben nicht die Absicht, nur Frauen oder nur Männer zu erfassen. Jede Form der Ungleichbehandlung ist ausgeschlossen.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

INHALTVERZEICHNIS

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

1 Vorwort

Die Bayerwald Media GmbH betreibt ein Managementsystem (auf Basis ISO 9001 ohne Zertifizierung). Risikomanagement (angelehnt an die ISO 27005) wurden berücksichtigt. Im Managementsystem wurde Informationssicherheit (angelehnt an die ISO 27001 ohne Zertifizierung) und Datenschutz (angelehnt an ISO 27701 ohne Zertifizierung) integriert. Regelmäßige Überprüfungen aller relevanten Prozesse, Verfahren, Arbeitsanweisungen findet statt. Verbesserungen werden in einem kontinuierlichen Verbesserungsprozess (KVP) erfasst, bewertet und ggf. dokumentiert durchgeführt. Ein Mitteilungsdienst informiert die Mitarbeiter/innen über Neuigkeiten und Änderungen. Der Mitteilungsdienst umfasst ebenfalls Kunden.

Das Dokument beschreibt die von der Geschäftsleitung als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang mit durchgeführten Auftragsverarbeitungsvorgängen zwischen Auftraggeber und Auftragnehmer. Die dargestellten Maßnahmen stellen somit ein Abbild des gelebten Datenschutzmanagementsystem der Bayerwald Media GmbH dar.

2 Geltungsbereich

Die beschriebenen technischen und organisatorischen Maßnahmen gelten für die Bayerwald Media GmbH.

3 Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 DSGVO.

Die DSGVO verpflichtet Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen.

Diese Anforderungen erfüllt der Auftragnehmer durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit.

Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- ☑ **Vertraulichkeit**: Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- ☑ **Integrität**: Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- ☑ **Verfügbarkeit**: Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- ☑ **Belastbarkeit**: Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst Widerstandsfähig ausgestaltet sein müssen.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

4 Vertraulichkeit

Geeignete technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit werden, unter Berücksichtigung des Stands der Technik, der Art, des Umfangs, der Umstände, dem Zweck der Verarbeitung, der Implementierungskosten, der unterschiedlichen Eintrittswahrscheinlichkeit, Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen. Hiermit wird ein dem Risiko angemessenes Schutzniveau gewährleistet.

4.1 Zutrittskontrolle

Unbefugten sind der Zutritt, Zugang und Zugriff zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

4.1.1 Objektsicherung

- ☑ Die Datenverarbeitungsanlagen befinden sich in einem von der Bayerwald Media GmbH angemieteten Räumen

4.1.2 Sicherheitszonen

- ☑ Sicherheitszonen wurden eingerichtet
- ☑ Die Datenverarbeitungsanlagen sind mit strikter Zutrittsbeschränkung und Überwachung zu versehen

4.1.3 Art der Zutrittskontrolle

- ☑ Die Schlüssel zu den Datenverarbeitungsanlagen besitzen nur bestimmte Personen
- ☑ Türsicherung
- ☑ Schlüsselregelung
- ☑ Schließregelung (verschlossene Türen bei Abwesenheit)

4.1.4 Regelung der Zutrittsberechtigungen

- ☑ Zutrittsregelungen zu den Datenverarbeitungsanlagen für Mitarbeiter
- ☑ Festlegung befugter Personen in den Räumen der Datenverarbeitungsanlagen
- ☑ Regelung beim Ausscheiden und Wechseln von Berechtigten
- ☑ Regelungen / Folgemaßnahmen bei Verlust von Schlüsseln usw.

4.1.5 Personenkontrolle

- ☑ Anmeldung und Begleitung von Besuchern und Firmenfremden

4.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

4.2.1 Regelung der Zugangsberechtigungen

- ☑ Regelungen für die Vergabe und Verwaltung von Zugangsberechtigungen
- ☑ Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- ☑ Zugangsberechtigte weisen sich durch Benutzerkennung und Passwort aus
- ☑ Authentisierung administrativer Zugriffe mit separaten Admin Accounts
- ☑ Zentrale Regelung der Verwendung von Passwörtern
- ☑ Regelung für Sperrung des Arbeitsplatzrechners beim Verlassen
- ☑ Berechtigungen (Kontenaktivierung) für temporäre Mitarbeiter/ Externe sind zeitlich befristet
- ☑ Zentrale Regelung beim Ausscheiden und Wechseln von Berechtigten
- ☑ Regelungen bei Verlust (Vergessen) des Passwortes
- ☑ Trennen der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen
- ☑ Getrennte Internet Infrastruktur für Besucher

4.2.2 Zusätzliche Maßnahmen beim Fernzugang

- ☑ Regelung für die Benutzung des Anschlusses, insbesondere bei Benutzung durch Dritte
- ☑ Festlegung der Personen, die zur Anmeldung von außerhalb befugt sind
- ☑ Netzzugangssicherungen durch Hard- und Softwaremaßnahmen (VPN-Zugänge)
- ☑ Verhinderung des unberechtigten Zugriffs aus dem Internet (Firewall)

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

4.2.3 Protokollierung von Zugängen

- ☑ Nachweis der Benutzung von IT-Systemen (Protokollierung der Zugänge)
- ☑ Protokollierung der fehlgeschlagenen Zugangsversuche (Entsperren eines Benutzers)
- ☑ Protokollierung der Vergabe / Änderung von Zugangsberechtigungen

4.3 Zugriffskontrolle / Benutzerkontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

4.3.1 Berechtigungskonzept

- ☑ Nachweis der Benutzung von IT-Systemen (Protokollierung der Zugänge)
- ☑ Protokollierung der fehlgeschlagenen Zugangsversuche (Entsperren eines Benutzers)
- ☑ Protokollierung der Vergabe/ Änderung von Zugangsberechtigungen

4.3.2 Zugriffsschutz

- ☑ Einsatz von Verschlüsselungsroutinen (speziell auch bei Passwortdateien)
- ☑ Trennung von Test- und Produktionsbetrieb
- ☑ Netzzugriffssicherungen

4.3.3 Aufbewahrung bei Verwendung von Datenträgern

- ☑ Zonen durch Zutrittskontrollsystem abgesichert
- ☑ Keine Reparatur von Datenträgern, sondern grundsätzlich Entsorgung und Vernichtung im Unternehmen
- ☑ Regelung der Vernichtung von Datenträgern in Abhängigkeit von der Art der Datenträger

4.3.4 Protokollierung von Zugriffen

- ☑ Protokollierung von Lese- und Schreibzugriffen auf die Datensicherungen
- ☑ Protokollierung der Vergabe von Zugriffen

4.4 Trennungskontrolle

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

- ☑ Logische Trennung der Daten
- ☑ Mandantenfähigkeit von Anwendungen (sofern erforderlich)
- ☑ Innerbetriebliche Vorgaben für die Datenerhebung und die -Verarbeitung

4.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne weitere Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen den entsprechenden technischen und organisatorischen Maßnahmen.
Umgesetzte Maßnahmen:

- ☑ Pseudonymisierung werden vom Auftragnehmer nur weisungsgebunden im Einzelfall realisiert.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

5 Integrität

Die Richtigkeit der verarbeiteten personenbezogenen Daten ist zu gewährleisten. Unzulässige Änderungen müssen identifiziert und korrigiert werden können.

5.1 Weitergabekontrolle

Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

5.1.1 Regelung der elektronischen Übertragung

- ☑ Festlegung der Personen, die zur Übermittlung befugt sind (Berechtigungskonzept)
- ☑ Verschlüsselung der Daten bei der Übertragung (SSL, verschlüsselte Mails, verschlüsselter Zugriff)
- ☑ Authentifizierung bei Mails
- ☑ Protokollierung der Datenübermittlung und der Empfänger

5.1.2 Regelung bei der Speicherung auf Wechseldatenträgern

- ☑ Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist grundsätzlich nicht vorgesehen
- ☑ Im Ausnahmefall werden ausschließlich verschlüsselte Datenträger verwendet

5.1.3 Regelungen des Transports von Datenträgern

- ☑ Transport von Datenträgern mit personenbezogenen Daten wird ausschließlich durch Betriebszugehörige durchgeführt
- ☑ Datenträger sind stets verschlüsselt

5.2 Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umgesetzte Maßnahmen:

- ☑ Zuständigkeiten für die Dateneingabe sind festgelegt (einschließlich Regelung der Stellvertretung)
- ☑ Dateneingaben sind durchgängig personalisiert und lückenlos auf den Anwender zurückzuführen.
- ☑ Externe Datenträger werden komplett gesperrt und können nicht verwendet werden.
- ☑ Jede/r Mitarbeiter/in hat ausschließlich auf die zur Aufgabenerfüllung notwendigen Daten Zugriff.

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

6 Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust abgesichert sind.

Umgesetzte Maßnahmen:

6.1 Erstellung und Verwahrung von Sicherheitskopien

- ☑ Generelles Datensicherungskonzept
- ☑ Kontrollierte und regelmäßige Sicherung der Benutzerdateien und Datenbanken
- ☑ Namenskonventionen für Sicherungsdateien
- ☑ Kennzeichnung der Datenträger
- ☑ Verwendung des Schreibschutzes bei Datenträgern
- ☑ Bestandsverzeichnis der Sicherungskopien gemäß Datensicherngskonzept
- ☑ Bestandskontrolle von Datenträgern
- ☑ Protokollierung von Sicherheitsspeicherungen
- ☑ Lagerung von Kopien an besonders geschützten Orten
- ☑ Festlegung von Aufbewahrungsfristen

6.2 Gewährleistung des laufenden Betriebes

Teile der Infrastruktur sind in einem Rechenzentrum ausgelagert. Der andere Teil wird in den Räumlichkeiten der Bayerwald Media GmbH betrieben.

- ☑ Riskomanagement wird regelmäßig betrieben
- ☑ Der laufende Betrieb ist durch technische und organisatorische Maßnahmen sichergestellt

6.2.1 Unterbrechungsfreie Stromversorgung

- ☑ Unterbrechungsfreie Stromversorgung mit ausreichender Kapazität ist den Datenverarbeitungsanlagen vorgeschaltet

6.2.2 Brandschutz

- ☑ CO^2-Handlöscher sind im Raum der Datenverarbeitungsanlagen vorhanden

6.2.3 Klimatisierung

- ☑ Rechenzentrum

6.2.4 Anbindung Internet

- ☑ Die Internetanbindung ist sowohl intern als auch für Gäste vorhanden
- ☑ Das interne W-LAN ist getrennt vom Gast W-LAN

6.3 Umgesetzte Maßnahmen zum betrieblichen Katastrophenschutz

- ☑ Mitarbeiterinformation zum Verhalten in Notfallsituationen besteht
- ☑ Mitarbeiter/innen werden regelmäßig geschult

6.4 Umgesetzte organisatorische Maßnahmen

- ☑ Zentrale und einheitliche Beschaffung
- ☑ Im Beschaffungsprozess von Hard- und Software werden Sicherheits- und Datenschutzaspekte berücksichtigt
- ☑ Arbeitsanweisungen, Verfahrens- und Prozessdokumentation für die wichtigsten Themenbereiche existieren, wurden verkündet und werden gelebt
- ☑ Es werden interne Audits nach Bedarf durchgeführt
- ☑ Die eingesetzte Hard- und Software wird regelmäßig überprüft
- ☑ Ein jährlicher IT-Jahresbericht informiert die Geschäftsleitung über den Stand

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM

7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1 Datenschutz-Management

Die umfangreichen Pflichten und Anforderungen der EU-DSGVO erfordern eine ganzheitliche Strategie nach einem strukturierten Ansatz und ein entsprechendes Managementsystem. Alle Elemente, die für die Sicherstellung des Datenschutzes erforderlich sind, unterliegen der systematischen Koordination des Managementsystems.

Umgesetzte Maßnahmen:

- ☑ Managementziele wurden erlassen
- ☑ Datenschutzmanagement wird betrieben und gelebt
- ☑ Arbeitsanweisungen, Verfahrens- und Prozessdokumentation für die wichtigsten Themenbereiche existieren, wurden verkündet und werden gelebt
- ☑ Es werden interne Audits nach Bedarf durchgeführt
- ☑ Mitarbeiter/innen werden regelmäßig geschult und sensibilisiert

7.2 Incident-Response-Management

Um im Bedarfsfall eines Vorfalls reagieren zu können, sind einschlägige Meldewege zu definieren und Verantwortlichkeiten festzulegen.

Umgesetzte Maßnahmen:

- ☑ Benutzeranweisung wurde erlassen
- ☑ Meldeprozess wird regelmäßig geschult
- ☑ Meldepflicht bei Datenpannen und Sicherheitsvorfällen wird regelmäßig geschult

7.3 Datenschutzfreundliche Voreinstellungen

Durch Voreinstellungen ist sicherzustellen, dass personenbezogene Daten nur nach den jeweiligen bestimmten Verarbeitungszweck verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit.

Umgesetzte Maßnahmen:

- ☑ Im Beschaffungsprozess von Hard- und Software werden Sicherheits- und Datenschutzaspekte berücksichtigt (Privacy by Default)
- ☑ Frühzeitige Einbindung des DSB bei allen Datenschutzthemen auch in Projekten (Privacy by Design)

7.4 Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers.

Umgesetzte Maßnahmen:

- ☑ Ein Verzeichnis aller AV-Verträge wird geführt
- ☑ Der AV-Vertrag regelt u.a. die Verpflichtung der Unterauftragnehmeer in gleicher Weise, die Möglichkit zur Kontrolle und Löschung der Daten
- ☑ Es besteht ein schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer
- ☑ Der Auftraggeber erteilt dem Auftragnehmer die Weisungen in Schriftform
- ☑ Der Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers
- ☑ Wenn beim Auftragnehmer eine Prüfung durch die Aufsichtsbehörde stattgefunden hat, so kann der Auftraggeber den Prüfbericht verlangen (gleiches gilt für Prüfungen bei möglichen Unterauftragnehmern)

Bayerwald Media GmbH
Kirchplatz 10
D-93482 Pemfling
+49 (0) 99 71 - 9 96 98-0
+49 (0) 99 71 - 9 96 98-29

Geschäftsführer
Wolfgang Brückl
Stefan Wistuba
info@bayerwaldmedia.de
www.bayerwaldmedia.de

HRB: 10845
Amtsgericht Regensburg
Steuer-Nr.: 211/122/10498
Ust.-ID.: DE 81 49 37 200

Sparkasse Cham
Kontonummer: 120 127 634
Bankleitzahl: 742 510 20
IBAN: DE66742510200120127634
BIC-Swift: BYLADEM1CHM