Datenschutzvereinbarung zur Sicherstellung der Konformität zum §11 Bundesdatenschutzgesetz (BDSG) für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag

§1 Gegenstand der Vereinbarung

Diese Vereinbarung regelt die Maßnahmen zur Sicherstellung der Durchführung der Vorschriften des §11 Bundesdatenschutzgesetzes (BDSG) bei der Datenverarbeitung im Auftrag, die sich aus der Beauftragung gemäß Ziffer 2.1. im Hinblick auf den Umgang mit personenbezogenen Daten ergeben. Der Auftrag umfasst Folgendes: Datenerhebung, -verarbeitung oder -nutzung (Kundendaten) im betriebsinternen Verwaltungsprogramm.

§2 Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenverarbeitung/ -erhebung/ -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber erteilt den Auftrag in schriftlicher Form. Änderungen des Vertragsgegenstandes und Verfahrensänderungen sind abzustimmen und entsprechend §1 Abs. 2.2 festzulegen. Der Auftraggeber hat das Recht, in folgendem Umfang Weisungen gegenüber dem Auftragnehmer zu erteilen: für den erfolgreichen Newsletter-Versand, Mündliche Weisungen sind unverzüglich in schriftlicher Form zu bestätigen.
Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner der Nachfolger bzw. der Vertreter in schriftlicher Form mitzuteilen. Falls Weisungen die unter §1 Abs. 2 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung des Ergebnisses der Auftragsleistung feststellt. Der Auftraggeber ist verpflichtet, alle im Rahmen des Auftragsverhältnisses erlangten Kenntnisse über technische und organisatorische Maßnahmen beim Auftragnehmer vertraulich zu behandeln. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang nach Maßgabe von §7 dieser Vereinbarung zu kontrollieren.

§3 Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu sperren oder zu löschen, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder Weisung verlangt. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt, es sei denn, sie sind zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich. Der Auftragnehmer erkennt die Datenherrschaft des Auftraggebers als Dateneigentümer an und übernimmt diesem gegenüber die Verantwortung, dass diese Daten ausschließlich für die in § 1 genannten Zwecke verwendet werden.
Es werden keine Datenträger angenommen. Der Auftragnehmer sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Verarbeitungsablaufs, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.
Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber zu büroüblichen Zeiten berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen dem Auftraggeber auszuhändigen. Sämtliche Datenträger des Auftragnehmers sind datenschutzgerecht sicher zu löschen, so dass keine weitere Nutzung oder eine Rückschluss auf die Daten mehr möglich sind. Test- und Ausschussmaterial ist unverzüglich datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe in schriftlicher Form zu bestätigen. Die Beauftragung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Bei einer Beauftragung von Unterauftragnehmern, deren Sitz sich nicht in der EU befindet, hat der Auftragnehmer sicherzustellen, dass mit den Unterauftragnehmern eine Datenschutzvereinbarung gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (Standardvertragsklauseln) abgeschlossen wird. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen und zu dokumentieren. Die Überprüfung von Daten ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtung nach § 11 BDSG und diese Vertragsbedingungen erfüllt hat. Die Unterauftragnehmer sind unter § 11 des Vertrages als Anlage aufzuführen. Die Verarbeitung und Nutzung der Daten findet ausschließlich 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 bedarf der Erfüllung der in den einschlägigen EU-Richtlinien getroffenen Regelungen, der Erfüllung gesetzlichen Regelungen nach dem Bundesdatenschutzgesetz und der vorherigen schriftlichen Zustimmung des Auftraggebers, und darf im Anschluss an diese Zustimmung nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind. Falls ein Subunternehmen beauftragt werden soll, gelten diese Anforderungen zusätzliche zu den Bestimmungen in § 3 Abs. 8 u. 9.
Die Sicherheit der Datenverarbeitung und die angewandten Verfahren gemäß § 9 BDSG sind mit dem Auftraggeber im Vorfeld abzustimmen.

§4 Beauftragter für den Datenschutz des Fördervereines Ihlsee Strandbad e.V.: Mark Röttger, Hauptstr.42, 23816 Bebensee, Email: om.roettger@gmail.com

Der Datentransport erfolgt immer in verschlüsselter und elektronischer Form.

§5 Datengeheimnis

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Verschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und sie auf das Datengeheimnis gemäß § 5 BDSG in schriftlicher Form verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.
Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Datensicherungsmaßnahmen nach der Anlage zu § 9 BDSG.
Für die auftragsgemäße Bearbeitung personenbezogener Daten nutzt der Auftragnehmer folgende Einrichtungen: Symantec Backup
Das separat beigefügte Datensicherheitskonzept (mit den Festlegungen entsprechend der Anlage zu § 9 BDSG) des Auftragnehmers wird als verbindlich festgelegt.
Der Auftragnehmer hat folgende Kontrollen oder zusätzliche Maßnahmen gemäß § 9 BDSG durchzuführen:
Der Auftragnehmer beachtet die Grundsätzliche ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverständnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind in schriftlicher Form zu vereinbaren, § 2 Abs.2 ist zu beachten. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten (§ 42a BDSG).

§6 Laufzeit

Diese Beauftragung gilt auf unbestimmte Zeit. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert.

§7 Haftung

Der Auftragnehmer haftet im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

§8 Sonstiges

Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht. Beide Seiten sind in diesem Fall verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.
Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Für Nebenabreden ist die Schriftform erforderlich. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
Gerichtsstand ist Bad Segeberg. Es gilt deutsches Recht.
Dieser Vertrag ist in 2 (zwei) Exemplaren, von denen jeder Vertragspartner eines erhält, ausgefertigt. Die Vertragspartner dürfen den Vertrag übersetzen, jedoch ist die deutsche Originalfassung maßgebend.

Anlagen zu Datenschutzvereinbarung im Auftrag:

A – Erläuterungen zu § 7 Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind. Rechtsgrundlage ist § 11 Abs. 2 BDSG, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach der Anlage zu § 9 BDSG erforderlichen Maßnahmen getroffen werden. Werden personenbezogene Daten verarbeitet, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. (Das Handbuch, in dem die Maßnahmen erläutert werden, kann auf Datenträgern beim BSI (www.bsi.de) bestellt werden.) Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Die Sicherheitsziele sind in der Anlage zu § 9 BDSG genannt. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertrag zu wiederholen.
Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, müssen die Maßnahmen im Vertrag vereinbart werden. Dabei sind wiederum die in der Anlage zu § 9 BDSG genannten Sicherheitsziele zu erreichen. Aus dem Katalog sollten die einzelnen Maßnahmen in den Vertrag übernommen werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog.

Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.

Abschottung von Netzen: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versucher erkannt werden. Technische Komponenten, die in Betracht kommen sind Firewalls, Intrusion Detection Systeme und ins besondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.

Abhörender Kommunikation: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten entsprechend dem Stand der Technik zu verschlüsseln.

Abmeldeprozeduren: Die Abmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

B – Beschreibung der technischen und organisatorischen Maßnahmen zu § 7 Datensicherungsmaßnahmen

Zutrittskontrolle: Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden: Kennwortschutz verschlüsselt

Zugangskontrolle: Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen: Verschlüsselungsverfahren entsprechend dem Stand der Technik

Zugriffskontrolle: Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können: Sicherungsmechanismen entsprechend dem Stand der Technik

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 das überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zu Datenübertragung vorgesehen ist. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Eingabekotrolle: Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind. Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens drei Jahre lang durch den Auftragnehmer aufbewahrt.

Verfügbarkeitskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Sicherungskopien des Datenbestandes werden in folgenden Verfahren hergestellt: hier Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und Aufbewahrungsort für Back-up-Kopien.

Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.