Mit Bezug auf die

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

> Datenschutzgrundverordnung <
(DSGVO)

(anwendbar seit 25. Mai 2018)

erstellt und beschließt die Geschäftsführung dieses Dokument als

> Technische und Organisatorische Maßnahmen <

gültig für den Verein ***Hafenwindmobil e.V.*** sowie die ***HBW Verwaltungs GmbH*** sowie alle verbundenen Unternehmen

nachfolgend „***Hafenwind***“ bzw. „***Hafenwind-Gesellschaften***“ genannt.

Dieses Dokument ist sowohl intern als Richtlinie zur Datenverarbeitung vereinbart, und soll gleichwohl für Mitglieder, Gesellschafter und Vertragspartner des Vereins / Unternehmens der Transparenz dienen.

Inhalt

Gemäß Artikel 5 der DSGVO gelten die

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Interne Festlegungen für Hardware, Speichermedien und Netzwerk

Nachfolgend werden allgemein alle digital (elektronisch) gespeicherten Dokumente und Dateien, welche auf den betrieblichen Servern und Speichermedien gespeichert sind und welche ggf. betrieblich-fachliche, vertragliche oder persönliche Inhalte haben können, als ***Daten*** bezeichnet.

Datensicherheit hat verschiedene Aspekte und bedeutet, geeignete Maßnahmen gegen die folgenden Gefahren und Risiken vorzusehen:

1. Datenverlust durch beschädigte Speichermedien (technische Fehler)
2. Datenverlust durch irrtümliche Löschung (Bedienungsfehler)
3. Datenverlust durch Sabotage z.B. durch „Hacker-Angriffe“ via Internet, infizierte Datenträger u.ä. (USB-Sticks, externe Festplattenlaufwerke, …)
4. Datenzugriff durch Unbefugte / Unberechtigte (Datendiebstahl).

Die Geschäftsführung der Hafenwind-Gesellschaften begegnet den o.g. Gefahren und Risiken mit den nachfolgend beschriebenen jeweiligen
Technischen und organisatorischen Maßnahmen (TOM) :

A. **Regelmäßige Datensicherung auf zwei externen Festplatten** mit USB-Anschluss, welche nach der Sicherungsmaßnahme stromlos feuer- und diebstahlgesichert verschlossen werden.
   Die Datensicherung erfolgt mindestens im monatlichen Rhythmus durch **Überschreiben / Hinzuschreiben der neuen Daten über die alten**.
   Hierbei wird diejenige Sicherungsfestplatte mit den jeweils älteren Daten aktualisiert, sodass bei etwaigem Verlust der Arbeitsdaten ein zweifaches Back-Up mit jeweils einem maximalen Alter von einem bzw. zwei Monaten vorhanden ist.
   Die Datensicherung erfolgt bei Bedarf häufiger / kurzfristiger, je nach Wichtigkeit bzw. Menge der hinzugekommenen / geänderten Daten.
B. **Arbeitsdaten** werden nur dann auf lokalen Festplatten der PCs / Notebooks gespeichert, wenn diese Rechner ausschließlich von der Geschäftsführung verwendet werden, keinen weiteren Benutzern zugänglich sind und passwortgeschützt sind, ansonsten erfolgt die Speicherung der Arbeitsdaten **auf einer externen Arbeits-Festplatte** (z.B. USB oder NAS). Der Zugriff auf die Verzeichnisse der externen Arbeits-Festplatte (und somit auf die darin befindlichen Dateien) ist ebenfalls passwortgeschützt – gleiches gilt für E-Mail-Daten, welche ggf. lokal durch die E-Mail-Client-Software gespeichert werden.
C. Alle Computer und Notebooks sind mit einer aktuellen und professionellen **Software gegen Hacker-Angriffe**, Viren, Trojaner u.ä. geschützt, (z.B. McAfee, Norton, F-Secure, …), welche regelmäßig und automatisch aktualisiert wird.
   Gleiches gilt für das jeweilige Betriebssystem des Rechners (Windows).
D. Die **Einstellung des Internet-Rooters** ist so eingerichtet, dass ein Zugriff von außerhalb via Internet auf Computer und betrieblichen Netzwerk-Festplatten nicht möglich ist. Da die Betriebsstätten der Geschäftsführung sich jeweils in den Privathäusern der Geschäftsführer befinden, wird durch die Netzwerk-Infrastruktur die Trennung zwischen privat und betrieblich gewährleistet.
   Das heißt: Es werden keine privaten Daten auf den betrieblichen Datenträgern / virtuellen Laufwerken gespeichert und umgekehrt.

E. Der **betrieblich genutzte „Cloud-Server“** zum Austausch zwischen der Geschäftsführung, der Buchhaltung und der Technischen Betriebsführung via Internet ist nur über eine Zugangsberechtigung mit Benutzername und Passwort (Login) zugänglich. Externe Benutzer (Buchhalter, Technische Betriebsführer, …) erhalten von der Geschäftsführung ein Login nach Unterzeichnung einer Geheimhaltungserklärung.
Die auf dem „Cloud-Server“ gespeicherten Daten werden wie die Daten der lokalen Arbeits-Festplatten gesichert – siehe A.

Interne organisatorische Festlegungen (Verhaltenskodex)

Dieser Abschnitt bezieht sich unter Beachtung der oben beschriebenen technischen Maßnahmen, welche auch bereits einige Verhaltensregeln beinhalten, insbesondere auf den Umgang mit sensiblen personenbezogenen Daten gemäß DSVGO.
Personenbezogene Daten werden abgegrenzt von betrieblichen / Firmen-Daten wie Bestellungen, Aufträge, Rechnungen, Dienstleistungs- und Lieferverträgen, welche zwischen der Firma und anderen Unternehmen (Business-to-Business) relevant sind, auch wenn hierin ggf. persönliche Ansprechpartner namentlich und mit betrieblichen Kontaktdaten enthalten sein können.
Personenbezogene Daten in diesem Sinne sind somit auf Privatpersonen bezogene Daten und Informationen, welche in Listen und Registern gespeichert sein können oder in digital gespeicherten Dateien und Dokumenten enthalten sein können.

Diese **Privatpersonen** können sein z.B.:
- Vereinsmitglieder / Gesellschafter
- Vertragspartner, Verpächter, Dienstleister und Lieferanten

Es werden ausschließlich die persönlichen Daten gespeichert, welche für die vertragliche Beziehung mit unserem Unternehmen bzw. unserer Gesellschaft relevant und erforderlich sind, so z.B.:
- Name und Adressdaten (Postanschrift, Telefon, Fax, E-Mail)
- Geburtsdatum und ggf. Geburtsname
- Bankverbindung und Steuernummer, Ausweis- / Führerschein-Nummer
- bei Gesellschaftern: Höhe bzw. Anteil der Geschäftsbeteiligung

Die betrieblich gespeicherten persönlichen Daten werden den betreffenden Personen nach Registrierung oder nach Änderung persönlich schriftlich mitgeteilt. Auf Anforderung können diese Personen über ihre o.g. gespeicherten persönlichen Daten jederzeit Auskunft anfordern.

Gespeicherte Dateien und Dokumente, welche persönliche Daten enthalten (gemäß o.g. Definition) **sind zusätzlich einzeln passwortgeschütz** und somit gegen unbefugten / unberechtigten Zugriff oder mitlesen gesichert – auch auf dem Übertragungswege, z.B. via E-Mail oder Internet-Upload zum Server / Download vom Server.

Hafenwind-Gruppe Friedrichskoog
Daniel Peters
(Datenschutzbeauftragter) Dezember 2022