1.1 Inhalt

2 Allgemeine Angaben

2.1 Datenschutz-Konzept

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte (Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1).
Datenschutz-Grundverordnung (https://www.jusline.at/gesetz/dsgvo)

2.2 Sachliche und räumliche Tätigkeit

Wir verarbeiten als Verein personenbezogene Daten von natürlichen Personen ab dem 6 Lebensjahr (Art 8 DSGVO) ganz oder teilweise automatisiert am Standort 2230 Gänserndorf,Sportgasse 12

3 Verfahrensverzeichnis

Referenzen: Art 30, Art 31 DSGVO, Erwägungsgründe Art 13, 75, 76, 82 und 89

3.1 Verantwortliche

Der Verantwortliche und für den Datenschutz Zuständige ist:

HLAVATY Michael, Bockflieserweg 17,2230 Gänserndorf
0676 75113041
Hlavaty.michael@gmail.com
Referenzen: Art 4 Z 7 DSGVO -5-

3.2 Mitglieder

3.2.1 Zweck

Verarbeitung und Übermittlung von Daten für die Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten

Die Mitgliederverwaltung umfasst die Aufnahme neuer, die Abrechnung bestehender und die Information von Mitgliedern. Hier werden regelmäßig persönliche Daten wie E-Mail Adresse, Kontodaten (falls die Beiträge per Bankeinzug eingezogen werden), Alter usw. erfasst.

Es werden persönliche Leistungsdaten die im Zuge des Trainings, Wettkampf oder Turniere erfasst und bei Bedarf an folgenden Empfänger weitergeleitet:

anderen nationalen Kegelverein
Österreichische Landesverbände
ÖSKB (Österreichische Sportkegler- und Bowlingverband)
WNBA (World Ninepin Bowling Association)

3.2.2 Rechtsgrundlagen

Die Rechtsgrundlage für die Verarbeitung ist eine Einwilligungserklärung oder eine berechtigte Interessen des Vereins (Anmeldeverfahren für Wettkämpfe).

- DSGVO Art 6
  - Absatz a) Einwilligung der Betroffenen,
  - Absatz b) zur Vertragserfüllung erforderlich
  - Absatz f) berechtigte Interessen des Verantwortlichen
- „SA003 Mitgliederverwaltung“ (siehe Standard- und Muster-Verordnung 2004)

3.2.3 Zustimmungserklärungen oder sonstige Unterlagen

Personen bezogene Daten und Zustimmungserklärungen sind unter Verschluss und nicht frei zugänglich aufbewahrt.

3.2.4 Kategorien der verarbeiteten Daten

- Vorlage ist die Standardanwendung „SA003 Mitgliederverwaltung“
- Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden, müssen auf Grund der konkreten Prüfung im Einzelfall gemäß Datenminimierung nach Art 5 Z 1 DSGVO mit der jeweiligen Nummer angegeben werden.

3.2.5 Verabeitungsverzeichnis

Siehe Dokument „Verabeitungsverzeichnis“

4 Impressum und Datenschutzerklärung

Nicht relevant

5 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

5.1 Vertraulichkeit

Im Verein ist ein besonderes Vertrauensverhältnis zu unseren Mitglieder, wir gehen daher mit allen erlangten Informationen verantwortungsbewusst um und wahren die Verschwiegenheit.

5.1.1 Zutrittskontrolle:

Der Zutritt zur Kegelbahn ist nur mit einem Schlüssel möglich
Das Büro (Kegelbahn) ist versperrt, wenn kein Vereinsmitglied anwesend ist.

5.1.2 Zugangskontrolle:

Schutz vor unbefugter Systembenutzung mit Kennwörter (unterschiedlichen Zeichenzusammensetzung, Mindestlänge 8 Zeichen, Regelmäßiger Wechsel, Erstanmeldeprozedur)

5.1.3 Zugriffskontrolle:

Nicht erforderlich

5.1.4 Klassifikationsschema für Daten:

Nicht erforderlich

5.2 Integrität

5.2.1 Weitergabekontrolle:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung.

5.2.2 Eingabekontrolle:

Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt.

5.3 Verfügbarkeit und Belastbarkeit

5.3.1 Verfügbarkeitskontrolle:

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Virenschutz und Firewall

5.3.2 Rasche Wiederherstellbarkeit;

Backup-Strategie

5.4 Pseudo-, Anonymisierung und Verschlüsselung:

Nicht erforderlich

5.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Ein Kontroll- und Verbesserungsprozess wir mindestens 1x jährlich durchgeführt

6 Betroffenenrechte wahren

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch (Art 21 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde

6.1 Prozesse betreffs Betroffenenrechte

- Wir erhalten Kenntnis dass ein Betroffener seine Rechte geltend machen will, sei es zB mündlich, schriftlich, per Email (h.schreiweis@aon.at).
- Sollte der Betroffene uns nicht persönlich bekannt sein, so müssen wir zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

  „Sehr geehrte Frau/Herr …! Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie zB Personen bezogene Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zukommen zu lassen. Ich danke Ihnen für Ihr Verständnis.

  Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten unsererseits sind notwendig.

Identität zweifelsfrei festgestellt: => Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 14 Tagen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:

Recht auf Auskunft (Art 15 DSGVO)
Der Betroffene bekommt als pdf sein Stammdatenblatt mit allen personenbezogenen Daten.

Recht auf Berichtigung (Art 16 DSGVO)
Der Betroffene bekommt als pdf sein Stammdatenblatt mit den berichtigten personenbezogenen Daten

Recht auf Löschung (Art 17 DSGVO)
Der Betroffene bekommt als pdf sein Stammdatenblatt ohne personenbezogene Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit den Hinweis, dass die Daten anonymisiert für die interne Statistik verwendet werden nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde

oder
Bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde wir alle Daten, bis auf jene, wo wir nach Art 6 Z 1 (f) ein berechtigtes Interessen des Verantwortlichen DSGVO (vor allem Buchhaltungsunterlagen) geltend machen können, löschen und daher aufgrund der gesetzlichen Aufbewahrungsfristen diese Daten auf jeden Fall erst nach 7 Jahre löschen; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die Personen bezogene Daten löschen. In diesen Fällen tritt an Stelle einer Löschung der Daten eine Sperrung (Einschränkung).

Recht auf Einschränkung (Art 18 DSGVO)
Der Betroffene bekommt als pdf sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Hackerl gesetzt ist und somit keine Verarbeitung seiner personenbezogenen Daten erfolgt.

Recht auf Übertragbarkeit (Art 20 DSGVO)
Der Betroffene bekommt als pdf sein Stammdatenblatt mit allen personenbezogenen Daten gemäß Art 20 Z2 DSGVO übermittelt und sein Stammdatenblatt mit allen personenbezogenen Daten als Cc.. an einen anderen Verantwortlichen, den der Betroffene uns genannt hat

Recht auf Beschwerde bei der Datenschutzbehörde

6.1.1 Profiling light
Nicht relevant

6.1.2 E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO)
Nicht relevant

6.2 Meldung von Datenschutzverletzungen
Die DSGVO definiert in Art 33 eine „Verletzung des Schutzes personenbezogener Daten“ (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

- Innerhalb von 72 Stunden mache wir eine Meldung mit Hilfe des „Datenschutzvorfall“ (siehe Anhang 8.1) an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes Personen bezogenen Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

- Gemäß Art 34 Z3 DSGVO muss keine Benachrichtigung der Betroffenen erfolgt, da die Verletzung des Schutzes Personen bezogenen Daten aufgrund meiner TOMs (zB Verschlüsselung in Rest und Motion, BackUp, …) voraussichtlich kein hohes Risiko für deren persönlichen Rechte und Freiheiten zur Folge hat.
- Wir werden alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 Z5 DSGVO.

7 Technische und organisatorische Maßnahmen TOMS

Die Ergriffenen Maßnahmen in unseren Unternehmen sind mit (X) angekreuzt.

7.1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☒ Manuelles Schließsystem
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Verschlossene Türen bei Abwesenheit

7.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ Zuordnung von Benutzerrechten
- ☒ Erstellen von Benutzerprofilen
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Einsatz von Anti-Viren-Software
- ☒ Einsatz einer Software-Firewall

7.1.3 Zugriffskontrolle

Maßnahmen, die 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 können.

- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

7.1.4 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.

- x Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- x E-Mail-Verschlüsselung
- x Verschlüsselung der übertragenen Daten

7.1.5 Eingabekontrolle

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

- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7.1.6 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

7.1.7 Trennungsgebot

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

- ☒ Erstellung eines Berechtigungskonzepts
- ☒ Festlegung von Datenbankrechten

7.1.8 Vertraulichkeit

- ❖ Zutrittskontrolle: Schutz vor unbefugtem Zutritt nur mit Schlüssel
- ❖ Zugangskontrolle: Schutz vor unbefugter Systembenutzung mit Kennwörter
- ❖ Zugriffskontrolle: Zugriff nur durch Verantwortlichen

7.1.9 Integrität

- ❖ Eingabekontrolle: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt.

7.1.10 Verfügbarkeit

- ❖ Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Virenschutz und Fire-wall
- ❖ Rasche Wiederherstellbarkeit: Backup

8 Risikoanalyse

Referenzen: Art 24 + Art 25 DSGVO, Erwägungsgründe: Art 74, 75, 76, 77, 78 und 81

8.1 Schutzbedarfsanalyse

Da es sich bei folgende Personen bezogene Daten der Mitglieder um Daten mit vernachlässigbaren bis geringem Schutzbedarf handelt, ist aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen vorhanden.

8.2 Risikoanalyse mit Maßnahmen

Schutzziele für meine Risikobewertung nach Art 4 Z 12 sind: Vertraulichkeit, Integrität und Verfügbarkeit. Die Risiko-Bewertung erfolgt nach „Schwere“ und „Eintrittswahrscheinlichkeit (EWK)“, siehe unten

Folgende Daten wurden analysiert und in die entsprechenden Kategorien eingetragen:

Kategorie	Personenbezogene Daten
1	Mitschriften u. Fotos
2	Bankverbindungen

Schwere	Existenzgefährdend				
	Wesentlich				
	Begrenzt		1, 2		
	Vernachlässigbar				
		Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert
		EWK			

8.3 Folgen der Maßnahmen betreffs Risiko

Data Breach		
Kein Risiko	Risiko	Hohes Risiko
	• Datenschutzbehörde informieren	
• Betroffene sind nicht zu informieren • Keine Folgenabschätzung notwendig		

Aufgrund der gesetzten TOMs muss bei einem DataBreach das betroffene Mitglied nicht informiert werden, nichts destotrotz wird die Behörde bei DataBreach mit Risiko für personenbezogene Daten der Kategorie 1 + 2 informiert.

Referenzen: Art 22 + 35 DSGVO, Erwägungsgründe: 76, 84 und 89 – 93, Working Paper 240 der Art 29 Gruppe

8.3.1 Bewertungsmaßstäbe

Schwere:

Schwere	Auswirkung auf Betroffene	Folgen überwinden	Beispiele
Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, …
Begrenzt	Wesentliche Unannehmlichkeiten	Unannehmlichkeiten sollten sich trotz Schwierigkeiten überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, …
Wesentlich	Wesentliche Folgen	Unannehmlichkeiten sollten sich trotz großer Schwierigkeiten überwinden lassen	Kategorien und Klassifizierungen werden bekannt, Missbrauch von Geldern, Vorladungen, Verschlechterung eines Verhältnisses, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte, …
existenz gefährdend	Irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	Bekanntwerden von Zahlungsverhalten und Bonität führen zu finanzielle Not; Betriebsgeheimniss und/oder vertrauliche Mitschriften werden Konkurrenz bzw. Öffentlichkeit bekannt und gefährden Betrieb; Identitätsdiebstahl; … langfristige Beschwerden, Tod, …

Eintrittswahrscheinlichkeit:

EWK	Wahrscheinlichkeit	Beispiele
Vernachlässigbar	0-24% Wahrscheinlichkeit	zB Diebstahl von Unterlagen aus einem Safe
Möglich	25-69% Wahrscheinlichkeit	Zb gezielter und koordinierter Angriff durch einen Hacker, Verlust des Hardware bzw pb Daten durch Diebstahl oder durch fahrlässiges Handeln
Sehr wahrscheinlich	70-99% Wahrscheinlichkeit	zB Eindringung eines Schädigungs-Mails,
Garantiert	100% Wahrscheinlichkeit garantiert	zB Ausfall durch einen Festplattenausfall, Datenverluste durch technische Fehler

8.4 Zusammenfassung

Wir sehe das hier dokumentierte Datenschutzniveau mit den gesetzten TOMs für unseren Verein auch aufgrund unserer finanziellen, technischen und organisatorischen Beschränkungen als **angemessen und ausreichend** an.

9 Anhang

9.1 Datenschutzvorfall gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018 (WKO)

Bitte senden Sie dieses Formular umgehend und vollständig ausgefüllt an die Geschäftsleitung:
HLAVATY Michael,
Bockflieserweg 17 2230 Gänserndorf
Telefon: 0676 75113041
E-Mail: hlavaty.michael@gmail.com

Tragen Sie hier die Kontaktinformationen des Datenschutzbeauftragten ein

1.	Detaillierte Sachverhaltsschilderung?		
2.	Wer ist Verantwortlicher?		
3.	Zeitraum oder Zeitpunkt des Vorfalls		
4.	Zeitpunkt der Feststellung des Vorfalls		
5.	Ursache des Vorfalls		
6.	Ort des Vorfalls		
7.	Art der Verletzung		
8.	Kategorien der betroffenen Personen		
9.	Anzahl der betroffenen Personen / betroffenen		
10.	Kategorien der personenbezogenen Daten		
11.	Sind besondere Kategorien personenbezogene Daten nach Art. 9 DSGVO betroffen? Falls ja: welche:	Ja ☐	Nein ☐
12.	Sind Daten zu Straftaten oder Ordnungswidrigkeiten betroffen? Falls ja: welche:	☐	☐
13.	Sind Bank-oder Kreditkartendaten betroffen? Falls ja: welche:	☐	☐
14.	Sind Bestands- und Nutzungsdaten im Bereich der Telemedien (z. B. Internet) wie beispielsweise Benutzererkennung und Passwörter betroffen? Falls ja: welche:	☐	☐
15.	Zu welchem Zweck wurden die in Ziffer 10 bis Ziffer 14 genannten Daten Verarbeitet? Falls ja: welche:	☐	☐
16.	Angaben zur Auftragsverarbeitung zur Durchführung der Verarbeitungstätigkeit werden Auftragsverarbeiter herangezogen: Falls ja: Benennen Sie die Auftragsverarbeiter	☐	☐

17.	Mögliche Folgen und Auswirkungen der Datenschutzverletzung für die betroffenen Personen ☐ Verlust der Kontrolle über ihre personenbezogenen Daten ☐ Einschränkung ihrer Rechte ☐ Diskriminierung, ☐ Identitätsdiebstahl oder -betrug ☐ finanzielle Verluste ☐ unbefugte Aufhebung der Pseudonymisierung ☐ Rufschädigung ☐ Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten ☐ andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person Ausführliche Beschreibung der möglichen Auswirkungen für die betroffenen Personen:		
18.	Erläuterung zu eingeleiteten Sicherheitsmaßnahmen bzw. geplanten Sicherheitsmaßnahmen nach dem Datenschutzvorfall, um die betroffenen Personen zu schützen		
19.	Erläuterung, in wie weit, die eingeleiteten Maßnahmen zu einer Minderung der nachteiligen Folgen für die betroffenen Personen führen		
20.	Erläuterung zu vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen des Verantwortlichen Die Daten sind verschlüsselt: Falls ja: Welcher Verschlüsslungsalgorithmus wurde verwendet: Falls nein: Nennen Sie andere technische und organisatorische Maßnahmen, die zum Schutz der in Ziffer 10 bis 14 genannten Daten ergriffen wurden:	Ja ☐	Nein ☐

Diesem Meldeformular sind folgende Anlagen beigefügt:

☐ Beschreibung der Verarbeitungstätigkeit aus Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO (Verantwortlicher)

☐ Beschreibung der Verarbeitungstätigkeit aus Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO (Auftragsverarbeiter)

☐ Dokumentation zur Datenschutz-Folgenabschätzung nach Art. 35 DSGVO

Ort, Datum	Vorname Nachname	Unterschrift