



Datenschutzordnung

Kanusportverein Wolfenbüttel e. V.

Beschlossen mit Vorstandsbeschluss vom 01.09.2026

§ 1 Zweck, Geltungsbereich und Abgrenzung

- (1) Diese Datenschutzordnung regelt den internen Umgang mit personenbezogenen Daten im Verantwortungsbereich des Kanusportvereins Wolfenbüttel e. V.
- (2) Sie gilt für Mitglieder der Vereinsorgane, Funktionsträger:innen, Übungsleiter:innen sowie alle sonstigen Personen, die im Auftrag des Vereins personenbezogene Daten verarbeiten.
- (3) Die Datenschutzinformation für Mitglieder erfüllt die Informationspflichten gegenüber betroffenen Personen. Das Verzeichnis der Verarbeitungstätigkeiten dokumentiert die einzelnen Verarbeitungsvorgänge; das Lösch- und Aufbewahrungskonzept enthält die Detailfristen und Löschereignisse. Diese Ordnung ersetzt keines dieser Dokumente.
- (4) Soweit andere Vereinsregelungen oder Einzelanweisungen den Datenschutz betreffen, ist diese Ordnung ergänzend anzuwenden. Gesetzliche Vorgaben gehen vor.

§ 2 Verantwortung und Datenschutzorganisation

- (1) Der Vorstand ist für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich. Er erteilt erforderliche Freigaben und Weisungen und sorgt für eine nachvollziehbare Dokumentation.
- (2) Der Vorstand legt für die operativen Datenschutzaufgaben zuständige Funktionen und Vertretungen fest. Dazu gehören insbesondere die Pflege der Datenschutzdokumentation, die Bearbeitung von Betroffenenanfragen, die Löschkontrolle und die Koordination bei Datenschutzvorfällen.
- (3) Personen, die Zweifel an Zweck, Rechtsgrundlage, Datenumfang, Empfängern oder Schutzmaßnahmen einer Verarbeitung haben, klären diese vor Beginn oder Fortsetzung der Verarbeitung mit dem Vorstand. Zentrale Kontaktstelle ist info@ksv-wf.de.
- (4) Die Voraussetzungen für die Benennung einer datenschutzbeauftragten Person werden bei wesentlichen Änderungen der Verarbeitung sowie bei gesetzlichen Änderungen erneut geprüft und dokumentiert.

§ 3 Grundsätze und Freigabe von Verarbeitungen

- (1) Personenbezogene Daten dürfen nur für einen vorher festgelegten, dokumentierten und rechtmäßigen Zweck verarbeitet werden. Umfang und Zugriff sind auf das für die jeweilige Aufgabe Erforderliche zu begrenzen.
- (2) Bei jeder Verarbeitung sind insbesondere Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit zu beachten. Eine private oder zweckfremde Nutzung von Vereinsdaten ist unzulässig.

- (3) Neue oder wesentlich geänderte Verfahren, Formulare, Dienste, Geräte oder Datenübermittlungen dürfen erst eingesetzt werden, nachdem der Vorstand sie geprüft und freigegeben hat. Vor der Inbetriebnahme sind erforderlichenfalls das Verzeichnis der Verarbeitungstätigkeiten, die Datenschutzinformation, Verträge und Schutzmaßnahmen anzupassen.
- (4) Daten besonderer Kategorien nach Art. 9 DSGVO dürfen nur verarbeitet werden, wenn sie für einen dokumentierten Zweck erforderlich sind, eine geeignete Rechtsgrundlage besteht und zusätzliche Schutzmaßnahmen festgelegt wurden. Nicht erforderliche Angaben werden nicht übernommen.

§ 4 Zugriffe, Berechtigungen und Vertraulichkeit

- (1) Zugriff erhalten nur Personen, die die jeweiligen Daten zur Erfüllung ihrer Aufgabe benötigen. Berechtigungen sind rollenbezogen, so gering wie möglich und zeitlich auf die Aufgabenwahrnehmung begrenzt zu vergeben.
- (2) Zugänge sind personenbezogen. Passwörter, Freigabelinks, Sicherheitscodes und sonstige Authentisierungsmittel dürfen nicht weitergegeben oder gemeinsam genutzt werden.
- (3) Der Vorstand führt oder veranlasst eine aktuelle Übersicht der vergebenen Berechtigungen. Freigaben, Änderungen und Entzüge werden dokumentiert und bei Aufgabenwechsel, Vertretungsänderung, Ausscheiden sowie in angemessenen Abständen überprüft.
- (4) Vor dem ersten Zugriff sind die betroffenen Personen nachweisbar auf Vertraulichkeit und weisungsgebundene Verarbeitung zu verpflichten. Die Verpflichtung gilt nach Ende der Tätigkeit fort.
- (5) Bei Ende oder Wechsel einer Aufgabe sind Unterlagen und Daten geordnet zu übergeben, nicht mehr benötigte lokale Kopien zu löschen und Zugänge unverzüglich anzupassen oder zu sperren.

§ 5 Freigegebene Systeme und Dienstleister

- (1) Vereinsdaten dürfen nur in vom Vorstand freigegebenen Systemen und Speicherorten verarbeitet werden. Nicht freigegebene private Cloud-Dienste, Apps oder Plattformen dürfen nicht verwendet werden.
- (2) Vor der Beauftragung eines Dienstleisters sind insbesondere Rollenverteilung, Auftragsvertragsvertrag, technische und organisatorische Maßnahmen, Verarbeitungsorte, Unterauftragnehmer und mögliche Drittlandübermittlungen zu prüfen und zu dokumentieren.
- (3) Wesentliche Änderungen an Produkten, Unterauftragnehmern, Speicherorten oder Vertragsbedingungen lösen eine erneute Prüfung aus. Erforderliche Anpassungen der Datenschutzinformation und des Verzeichnisses der Verarbeitungstätigkeiten sind vor oder unverzüglich nach Wirksamwerden vorzunehmen.
- (4) Die konkret eingesetzten Anbieter und mitgliederbezogenen Transparenzangaben werden nicht in dieser Ordnung wiederholt, sondern in den jeweils dafür vorgesehenen Primärdokumenten geführt.

§ 6 E-Mail und Dokumentenübermittlung

- (1) Für Vereinsaufgaben sind vorhandene dienstliche beziehungsweise vereinsbezogene E-Mail-Konten zu verwenden. Die Nutzung privater Konten bedarf einer ausdrücklichen Freigabe und geeigneter Schutzmaßnahmen.

- (2) Bei Rundschreiben werden Empfängeradressen grundsätzlich über das BCC-Feld geschützt, sofern die gegenseitige Sichtbarkeit nicht für den konkreten Zweck erforderlich und rechtmäßig ist.
- (3) Vertrauliche Einzelangelegenheiten werden nur an die betroffene beziehungsweise zuständige Person versandt. Bank-, Zahlungs-, Gesundheits-, Ausweis- und Ermäßigungsnachweise dürfen nicht über ungeschützte Gruppenverteiler übermittelt werden.
- (4) Vor dem Versand sind Empfänger, Anhänge, Freigabelinks und Datenumfang zu prüfen. Fehlversand oder irrtümliche Freigaben sind unverzüglich als möglicher Datenschutzvorfall zu melden.

§ 7 Information bei Dritterhebung

- (1) Erhält der Verein personenbezogene Daten nicht unmittelbar von der betroffenen Person, stellt er dieser die jeweils aktuelle Datenschutzinformation grundsätzlich selbst bereit.
- (2) Die Information erfolgt grundsätzlich innerhalb eines Monats, spätestens jedoch bei der ersten Kommunikation mit der betroffenen Person oder vor der ersten Offenlegung an Dritte. Gesetzliche Ausnahmen sind zu prüfen und zu dokumentieren.
- (3) Volljährige Familienmitglieder werden unmittelbar durch den Verein informiert. Bei Minderjährigen wird die Information den gesetzlichen Vertretungen bereitgestellt. Eine zusätzliche Weitergabe durch die antragstellende Person bleibt möglich.
- (4) Version, Datum, Versandweg und Ergebnis der Bereitstellung werden dokumentiert. Nicht zustellbare Informationen sind nachzuverfolgen. Der Vorstand legt hierfür die zuständige Funktion und den verbindlichen Ablauf fest.

§ 8 Nachweise für Beitragsermäßigungen

- (1) Erforderliche Nachweise für Beitragsermäßigungen sind von den betroffenen Mitgliedern unaufgefordert einzureichen; der Übermittlungsweg ist nicht vorgegeben. Nur ausnahmsweise fragt der Kassenwart vor der Abrechnung nach.
- (2) Nach Abschluss der Prüfung wird eine eingereichte Kopie gelöscht oder zurückgegeben. Gespeichert werden nur Nachweisart, ausstellende Stelle, Gültigkeit, Prüfdatum und prüfende Funktion.

§ 9 Übermittlungen an Verbände und öffentliche Stellen

- (1) Übermittlungen erfolgen nur, wenn Zweck, Rechtsgrundlage, Datenumfang und Empfänger im Verzeichnis der Verarbeitungstätigkeiten dokumentiert sind. Es werden nur die für den jeweiligen Zweck erforderlichen Daten übermittelt.
- (2) Die jährliche Bestandserhebung an den LandesSportBund Niedersachsen e. V. wird in der in der Datenschutzinformation beschriebenen aggregierten Form vorbereitet, auf Plausibilität geprüft, freigegeben und mit einem Übermittlungsnachweis dokumentiert.
- (3) Weitere Meldungen, etwa für Lizenzen, Wettkämpfe oder Versicherungsfälle, werden vor der ersten Übermittlung gesondert geprüft. Erforderliche Transparenzinformationen sind vorab zu ergänzen.
- (4) Bei Auskunfts- oder Übermittlungsverlangen öffentlicher Stellen sind Zuständigkeit, Rechtsgrundlage und Umfang zu prüfen. Zweifel werden vor der Herausgabe mit dem Vorstand geklärt.

§ 10 Fotos, Videos und Veröffentlichungen

- (1) Vor der Aufnahme oder Veröffentlichung personenbezogener Fotos und Videos werden Zweck, Medium, Empfängerkreis, Reichweite, vorgesehene Dauer und Rechtsgrundlage festgelegt.
- (2) Soweit eine Einwilligung erforderlich ist, wird sie getrennt, freiwillig, verständlich und nachweisbar eingeholt. Diese Ordnung ersetzt keine Einwilligungserklärung und begründet für sich allein keine Veröffentlichungsbefugnis.
- (3) Veröffentlichungen im Namen des Vereins erfolgen nur über freigegebene Kanäle und durch hierzu berechtigte Personen. Private Konten dürfen nicht ohne Freigabe als Vereinskanal genutzt werden.
- (4) Widerrufe, Widersprüche und Löschanfragen werden unverzüglich an die zuständige Stelle weitergeleitet. Inhalte werden nach Prüfung soweit möglich entfernt oder in ihrer Nutzung eingeschränkt; die Bearbeitung wird dokumentiert.

§ 11 Private Geräte und Sicherheit

- (1) Private Endgeräte dürfen für Vereinsdaten nur mit ausdrücklicher Freigabe des Vorstands und nur dann genutzt werden, wenn ein dem Risiko angemessenes Schutzniveau gewährleistet ist.
- (2) Erforderlich sind insbesondere ein wirksamer Geräte- und Bildschirmschutz, aktuelle Sicherheitsupdates, angemessene Verschlüsselung sowie eine Trennung von Vereins- und Privatnutzung. Sicherheitsfunktionen dürfen nicht umgangen werden.
- (3) Vereinsdaten werden nicht dauerhaft lokal, in privaten Backups, privaten Cloud-Speichern oder auf nicht freigegebenen Wechseldatenträgern abgelegt. Arbeitskopien sind nach Übertragung in das freigegebene Vereinssystem zu löschen.
- (4) Verlust, Diebstahl, Schadsoftware, unbefugter Zugriff oder eine sonstige Beeinträchtigung eines genutzten Geräts sind unverzüglich zu melden. Bis zur Klärung darf das Gerät nicht weiter für Vereinsdaten eingesetzt werden.

§ 12 Aufbewahrung, Löschung und Entsorgung

- (1) Aufbewahrungsfristen und Löschereignisse ergeben sich aus dem Verzeichnis der Verarbeitungstätigkeiten und dem freigegebenen Lösch- und Aufbewahrungskonzept. Diese Ordnung wiederholt die Detailfristen nicht.
- (2) Der Vorstand legt für die betroffenen Systeme und Papierbestände Löschverantwortung, Vertretung, Kontrollrhythmus und Nachweisform fest.
- (3) Nach Eintritt eines Löschereignisses sind Daten aus den maßgeblichen Systemen, E-Mail-Verteilern, Gruppenlisten, lokalen Arbeitskopien und Papierbeständen zu entfernen oder sicher zu vernichten. Gesetzlich weiter aufzubewahrende Daten werden gesperrt und im Zugriff beschränkt.
- (4) Löschläufe, begründete Zurückstellungen und die sichere Entsorgung schutzbedürftiger Unterlagen oder Datenträger werden nachvollziehbar dokumentiert.

§ 13 Betroffenenanfragen und Datenberichtigung

- (1) Anfragen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch oder Widerruf werden unverzüglich an die vom Vorstand festgelegte Datenschutzkontaktstelle weitergeleitet.
- (2) Eingangsdatum, Identitätsprüfung, Gegenstand und gesetzliche Bearbeitungsfrist werden dokumentiert und überwacht. Auskünfte werden nur nach angemessener Identitätsprüfung erteilt.

- (3) Die zuständige Stelle ermittelt die betroffenen Systeme, Unterlagen, Dienstleister und Empfänger, koordiniert erforderliche Maßnahmen und lässt die Antwort vor Versand freigeben.
- (4) Berichtigungen, Löschungen und Einschränkungen sind in allen betroffenen Beständen umzusetzen. Soweit erforderlich, werden Empfänger informiert; Umsetzung und Ergebnis werden dokumentiert.

§ 14 Datenschutzvorfälle

- (1) Mögliche Datenschutzverletzungen sind unverzüglich dem Vorstand über info@ksv-wf.de zu melden. Dazu zählen insbesondere Fehlversand, Verlust von Geräten oder Unterlagen, unberechtigter Zugriff, Schadsoftware, versehentliche Veröffentlichung und unzulässige Löschung oder Veränderung.
- (2) Soweit gefahrlos möglich, sind weitere Offenlegungen zu stoppen, Zugänge zu sperren und Beweise zu sichern. Eigenständige externe Mitteilungen oder die Vernichtung relevanter Nachweise unterbleiben, sofern sie nicht zur unmittelbaren Schadensbegrenzung erforderlich sind.
- (3) Der Vorstand bewertet Risiko und Meldepflicht, dokumentiert den Vorfall und veranlasst gegebenenfalls die Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden. Bei voraussichtlich hohem Risiko werden betroffene Personen nach Art. 34 DSGVO benachrichtigt.
- (4) Alle beteiligten Personen und Dienstleister stellen die für Bewertung, Abhilfe und Dokumentation erforderlichen Informationen unverzüglich bereit.

§ 15 Unterweisung, Kontrolle und Aktualisierung

- (1) Personen mit Zugriff auf Vereinsdaten werden vor Aufnahme ihrer Tätigkeit und anschließend anlassbezogen zu den für ihre Aufgabe geltenden Datenschutz- und Sicherheitsregeln unterwiesen.
- (2) Der Vorstand überprüft die Wirksamkeit der organisatorischen und technischen Maßnahmen mindestens einmal jährlich sowie anlassbezogen anhand einer dokumentierten Checkliste. Festgestellte Mängel werden dokumentiert und nachverfolgt.
- (3) Änderungen von Rechtslage, Vereinsorganisation, Verfahren oder IT-Diensten werden darauf geprüft, ob diese Ordnung und die zugehörigen Datenschutzdokumente angepasst werden müssen.
- (4) Bei Verstößen können Berechtigungen bis zur Klärung eingeschränkt oder entzogen und weitere nach Satzung, Ordnung oder Gesetz zulässige Maßnahmen ergriffen werden.

§ 16 Beschluss und Inkrafttreten

- (1) Diese Datenschutzordnung wird vom Vorstand auf Grundlage seiner satzungsmäßigen Zuständigkeit für Vereinsordnungen beschlossen.
- (2) Sie tritt mit Beschluss des Vorstands in Kraft.
- (3) Änderungen dieser Ordnung bedürfen eines Vorstandsbeschlusses. Rein redaktionelle Berichtigungen ohne Regelungsänderung werden nachvollziehbar dokumentiert.