



# **Datenschutzordnung**

**Berliner Kanu-Club „Borussia“ e.V.**

**Scharfenberger Straße 50  
(Schwarzer Weg)  
13505 Berlin**

**Neufassung vom 15.02.2019**

## **§ 1 Rechtsgrundlage der Datenverarbeitung**

- (1) Zur Erfüllung der Zwecke und Aufgaben des Vereins werden unter Beachtung der gesetzlichen Vorgaben des Datenschutzgesetzes (DSGVO, BDSG-neu) personenbezogene Daten über persönliche und sachliche Verhältnisse der Mitglieder im Verein verarbeitet, d. h. genutzt, gespeichert, übermittelt und verändert.

## **§ 2 Datenschutzverantwortung**

- (1) Die Datenschutzverantwortung für die Verwaltung der Mitgliederdaten liegt beim Geschäftsführenden Vorstand nach § 26 Abs. 1 Satz 2 BGB, da weniger als 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Er muss die ordnungsgemäße Anwendung der Datenverarbeitung überwachen und die mit der Verarbeitung befassten Personen mit den Vorschriften des Datenschutzes vertraut machen. Weiterhin stellt er den ordnungsgemäßen Umgang mit den Daten durch technische und organisatorische Maßnahmen sicher.

## **§ 3 Verpflichtung zur Vertraulichkeit**

- (1) Alle Vorstandsmitglieder und alle sonstigen Funktionsträger, denen zur Erfüllung ihres Aufgabengebiets personenbezogene Daten zur Verfügung gestellt werden, müssen schriftlich zur Vertraulichkeit verpflichtet werden. Demnach dürfen personenbezogene Daten der Mitglieder ohne deren ausdrücklich erklärtes Einverständnis Dritten (z. B. auch anderen Mitgliedern!) gegenüber nicht bekannt gemacht werden. Sie haben die gesetzlichen Vorgaben und diese Datenschutzordnung unbedingt zu beachten.

## § 4 Erhebung von personenbezogenen Daten

- (1) Zur Erfüllung seines geschäftsmäßigen Zwecks erhebt der Verein als **Pflichtangaben** folgende personenbezogenen Daten beim Eintritt seiner Mitglieder:

*Name, Anschrift, Geburtsdatum, Name des Erziehungsberechtigten (bei Minderjährigen), Geschlecht, Mitgliedsstatus, Eintrittsdatum*

- (2) Weiterhin erhebt er folgende **freiwillige Angaben**:

*E-Mail-Adresse, Telefonnr., Mobilfunknr., Zustimmung zu Veröffentlichungen von Bildern und Starter- und Ergebnislisten in div. Medien (z. B. Internetpräsenz, Social Media, Schwarzes Brett, Lokalpresse...)*

Die Genehmigung zur Verarbeitung freiwilliger Angaben kann jederzeit schriftlich durch das Mitglied widerrufen werden.

- (3) Im Rahmen von Sportveranstaltungen werden personenbezogene Daten von Teilnehmern nach Maßgabe der Notwendigkeit zur erfolgreichen Durchführung der Veranstaltung erhoben und verarbeitet. Die Teilnehmer haben demzufolge auch die gleichen Rechte u. a. auf Einhaltung der Datenschutzmaßnahmen wie die Vereinsmitglieder.

## § 5 Übermittlung von personenbezogenen Daten

- (1) Als Verbandsmitglied darf der Verein satzungsgemäß folgende Daten an den LKV Berlin e.V., Eisenhammerweg 22 A, 13507 Berlin, übermitteln:

*Geschlecht, Name, Geburtsdatum, Stammverein, Mitgliedsstatus*

- (2) Als Mitglied des Bezirkssportbundes Reinickendorf darf der Verein satzungsgemäß folgende Daten an den BSB Reinickendorf e.V., Eichborndamm 215-239, 13437 Berlin, übermitteln:

*Name, Geburtsdatum*

- (3) Für den Mitgliedsausweis (Ausweis und Einkaufsvorteile) übermittelt der Verein im freiwilligen Einvernehmen mit dem Mitglied folgende Daten an die DSA Deutsche Sportausweis GmbH, Massenbergstraße 9-13, D-44787 Bochum ([www.sportausweis.de](http://www.sportausweis.de))

*Name, Adresse, Geburtsdatum, Verein, Funktion, Mitgliedsnummer*

- (4) Jede weitere Übermittlung an Dritte bedarf der schriftlichen Einwilligung des Mitglieds. Dies betrifft insbesondere auch die Speicherung in privaten Speichermedien (z. B. Smartphones, Tablets usw.), da hier oftmals „unbewusste“, aber dennoch illegale Übermittlungen an Dritte durch Programme (z. B. WhatsApp, vgl. § 7 (10)) stattfinden.
- (5) Für die Verarbeitung personenbezogener Daten ist die Verwendung der unter dem Namen „cloud“ und „cloud computing“ bekannten IT-Dienstleistungen, wie externer Speicherplatz (z. B. Onedrive, Dropbox o. ä.) und Anwendungssoftware im Internet (z. B. Office 365), nicht gestattet, da dem Verein bei den hierbei bekannten Risiken sowohl die Kapazitäten als auch die Kompetenzen fehlen, die Einhaltung des Datenschutzes einzuschätzen bzw. zu überwachen.
- (6) Auf der Homepage des Vereins *bkc-borussia.de* werden die Vor- und Zunamen von Vorstandsmitgliedern mit einem Porträtbild und der ihrem Funktionsbereich zugeordneten E-Mail-Adresse veröffentlicht.
- (7) Die Veröffentlichung von Bildern und Videoaufnahmen von Sportveranstaltungen sind nur insoweit zulässig, als dadurch keine berechtigten Interessen der abgebildeten Personen verletzt werden. Einzelfotos dürfen nur nach ausdrücklicher, aber widerrufbarer Zustimmung der abgebildeten Person veröffentlicht werden. Wann immer möglich, sollten in Berichten nur Vornamen genannt werden. Ausnahmen stellen die Veröffentlichungen besonderer sportlicher Leistungen dar, in denen neben dem vollständigen Namen auch Jahrgang und Geschlecht des Mitglieds (soweit wertungsrelevant) genannt werden dür-

fen. In jedem Fall ist immer sorgfältig zwischen den Interessen des Mitglieds und denen des Vereins abzuwägen.

## **§ 6 Betrieb von Internetseiten**

- (1) Zuständig für die Veröffentlichung und Änderung von Internetseiten sowie die Einhaltung der diesbezüglichen rechtlichen Vorschriften sind der/die Medienwart/in und die von ihm weisungsabhängigen Beauftragten (z. B. Redakteure usw.).
- (2) Die Einrichtung von eigenen, aber vereinsbezogenen Internetseiten (auch in Sozialen Medien) muss vom Geschäftsführenden Vorstand bis zum Widerruf genehmigt werden. Die Betreiber sind dem Medienwart gegenüber weisungsabhängig und für die Einhaltung aller rechtlichen Vorschriften verantwortlich. Zugangsdaten sind dem Medienwart auszuhändigen.

## **§ 7 Technische und organisatorische Datenschutzmaßnahmen**

- (1) Die Mitgliederverwaltung und Buchhaltung werden mithilfe eines kommerziellen Vereinsverwaltungsprogramms ausschließlich auf zwei vereinseigenen, räumlich voneinander getrennten Rechnern ausgeführt. Diese sind mit Zugangskennungen und Verschlüsselungstechniken gegen den Zugriff unberechtigter Personen geschützt. Es werden regelmäßig Datensicherungen auf ebenfalls verschlüsselten Datenträgern vorgenommen. Die Synchronisation der beiden Arbeitsplätze erfolgt über einen TLS-verschlüsselten Datentransfer über den E-Mail-Dienst des Internets.
- (2) Daten dürfen immer nur im Rahmen der zwingenden Notwendigkeit erfasst werden (Datenvermeidung und -sparsamkeit). Den Funktionsträgern dürfen nur die Daten zugänglich gemacht werden, die für ihren Funktionsbereich zwingend erforderlich sind.
- (3) Datensicherheit auf dem Rechner ist zu beachten. Auf Privatrechnern ist ein separater Bereich für Vereinszwecke einzurichten. Der Zugang zu diesem Bereich ist durch ein möglichst

sicheres Kennwort vor dem Zugriff durch unautorisierte Personen (z. B. Freunde, Familienmitglieder usw.) zu schützen. Der Vereinsbereich und/oder die Daten sind mithilfe geeigneter Software und ebenfalls sicherem Kennwort zu verschlüsseln. Dokumente mit personenbezogenen Daten dürfen nicht offen zugänglich sein.

- (4) Bei Internetanschluss des Rechners (über LAN oder WLAN) sind zumindest grundlegende, zumutbare und dem jeweiligen Stand der Technik entsprechende Sicherheitsmaßnahmen zu treffen. Virenschutzprogramm und Software-Firewall sind unerlässlich, da sonst Daten von etwaigen Angreifern ausspioniert werden können. Etwaige Sicherheitsaktualisierungen des Betriebssystems und der Programme sind regelmäßig und zeitnah durchzuführen.
- (5) Bei Datenübermittlungen per WLAN muss die WLAN-Verbindung mit dem höchsten Sicherheitsstandard, geschützt sein, mindestens jedoch mit dem WPA2-Standard.
- (6) Datensicherungen sind regelmäßig durchzuführen; externe Sicherungsmedien (USB-Stick, CD, DVD, externe Festplatte, usw.) müssen sicher verschlüsselt und unter Verschluss aufbewahrt werden.
- (7) E-Mail-Austausch darf ausschließlich über SSL/TLS-verschlüsselte Verbindungen erfolgen. Vereinskommunikation über E-Mail muss immer mit Adressierung im BCC-Modus erfolgen, sobald mehr als ein Empfänger angeschrieben wird. Zentrale E-Mail-Verteiler über die Vereinsdomain (z. B. *mitglieder@bkcborussia.de*) sind leichter zu verwalten als lokale Adresssammlungen und zur Vermeidung von Adressierungsfehlern zu bevorzugen.
- (8) Bei Aufgabe von Ämtern oder Funktionen sind alle Daten dem/der Nachfolger/in zu übergeben und auf dem PC sicher, d. h. nicht wiederherstellbar zu löschen. Daten auf Papier sind vollständig zu übergeben, nicht mehr benötigte Dokumente sind im Papierschredder zu entsorgen.

- (9) Speichermedien sind im Falle eines Defekts vor der Entsorgung unrettbar zu zerstören. Keinesfalls dürfen Unterlagen auf Dachböden, Kellern oder in der Papiersammlung entsorgt werden.
- (10) Besonderes Augenmerk ist auf die Verwendung von Programmen zur Organisation zu legen. Werkzeuge wie z. B. WhatsApp verlangen bei der Installation/Einrichtung Zugriff auf das komplette Telefonbuch, das dann ohne weitere Rückfrage zum Hersteller (hier Facebook) übertragen wird. Hat man beispielsweise unerlaubt, also ohne schriftliche Einwilligung, Daten der Mitglieder seiner Trainingsgruppe (Name / Adresse/ Tel.nr usw.) im Telefonbuch seines Smartphones gespeichert, erfüllt das neben dem Verstoß gegen den Grundsatz der Datenvermeidung und -sparsamkeit den Tatbestand einer unerlaubten Übermittlung an Dritte. Wenn man nicht auf den Einsatz eines solchen Programms verzichten kann, müssen die schriftlichen Zustimmungen der Betroffenen zur Datenübertragung an den Programmbetreiber eingeholt, nur so wenig Daten wie irgend nötig gespeichert, sowie Pseudonyme verwendet werden.

## **§8 Informations-, Auskunfts- und Widerrufsrecht, Recht auf Berichtigung, Sperrung und Löschung**

- (1) Jedes Mitglied hat ein Recht darauf zu erfahren, welche Daten der Verein von ihm gespeichert hat. Die Daten sind ihm zeitnah in maschinenlesbarer Form auszuhändigen.
- (2) Jedes Mitglied kann die Erlaubnis zur Verarbeitung von auf seine Person bezogenen Daten widersprechen, es sei denn, diese sind zur Erfüllung des geschäftsmäßigen Zwecks des Vereins unbedingt notwendig.
- (3) Jedes Mitglied kann verlangen, dass falsche Daten über seine Person zeitnah korrigiert werden.
- (4) Bei Austritt hat das Mitglied ein Recht darauf, dass seine Daten zur Weiterverwendung gesperrt werden. Sie werden für die gesetzlich vorgeschriebenen Fristen archiviert und sicher auf-

bewahrt. Nach Ablauf der Fristen sind die Daten restlos zu löschen, es sei denn, der Verein hat ein Interesse zur teilweisen Aufbewahrung für vereinshistorische Zwecke.

## **§ 9 Inkrafttreten**

- (1) Diese Datenschutzordnung tritt gemäß Beschluss der Mitgliederversammlung vom 03.03.2019 in Kraft.