FC INDE HAHN e.V.

Datenschutzordnung

Inhaltsverzeichnis

Präambel 2
§ 1. Personenbezogene Daten werden erhoben, verarbeitet und genutzt 2
§ 2. Daten werden an Dritte übermittelt 3
§ 3. Verpflichtung auf das Datengeheimnis ist obligatorisch 4
§ 4. Mitglieder können Nutzung ihrer Daten freiwillig zustimmen 4
§ 5. Bestellung eines Vereinsdatenschutzbeauftragten 5
§ 6. Grenzen des Datenschutzes durch den Verein 6
§ 7. Inkrafttreten 6
Anlagen 7
Anlage 1: Technische und organisatorische Maßnahmen zum Schutz von Daten 7
Anlage 2: Verpflichtung auf das Datengeheimnis (§5 BDSG) 10
Anlage 3: Merkblatt zur Verpflichtung auf das Datengeheimnis 11
Anlage 4: Datenschutzrechtliche Einwilligungserklärung .....
Anlage 5: Verfahrensverzeichnis für automatisierte Verfahren zur Datenverarbeitung .....
Anlage 6: Glossar: .....

FC INDE HAHN e.V.

Präambel

Zur Pflege und Förderung des Sports (Zweck des Vereins) und allen damit unmittelbar und mittelbar in Zusammenhang stehenden Aufgaben ist es für den „FC Inde Hahn e.V.“ (im Folgenden „Verein“ genannt) notwendig, personenbezogene Daten seiner Mitglieder zu erheben, zu verarbeiten und weiterzugeben.
Damit der Verein das Grundrecht auf informationelle Selbstbestimmung seiner Mitglieder (im Folgenden auch „Betroffene“ genannt) bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten angemessen berücksichtigt, gibt sich der Verein gemäß § 21 Abs. 4 der Vereinssatzung folgende Datenschutzordnung.

§ 1

Personenbezogene Daten werden erhoben, verarbeitet und genutzt

Mitglieder

Von allen Mitgliedern (und ihren gesetzlichen Vertretern) werden personenbezogene Daten erhoben, verarbeitet und genutzt, um den ordnungsgemäßen Ablauf des Vereinsbetriebs sicherzustellen und den Vereinszweck zu erfüllen. Der Verein handelt dabei nach dem Grundsatz der Datenvermeidung und Datensparsamkeit, das heißt es werden nur so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt.

Zum Schutz der Persönlichkeitsrechte werden die Daten ehemaliger Mitglieder inaktiv gestellt.

Sportler

Von Mitgliedern, die im Verein sportlich tätig sind oder waren werden Daten erhoben, verarbeitet und genutzt, die im Zusammenhang mit ihrer sportlichen Aktivität stehen (z. B. Spielerpassnummer).
Daten über die Leistung und das soziale Verhalten von Sportlern werden erhoben, verarbeitet und genutzt, um den Vereinszweck zu erfüllen (insbesondere Durchführung eines leistungsorientierten Trainingsbetriebes).
Daten über die Gesundheit von Sportlern werden nur dann erhoben, verarbeitet und genutzt, wenn eine ausdrückliche, schriftliche Einwilligung des Betroffenen vorliegt.
Bei ausländischen Spielern werden aus verbandsrechtlicher Sicht weitere Daten erhoben, verarbeitet und genutzt, die im Zusammenhang mit einer inländischen Spielberechtigung stehen.

Funktionsträger

Von Mitgliedern, die Aufgaben innerhalb des Vereins erfüllen (Vorstand, Trainer, Betreuer, etc.) werden weitere Daten erhoben, verarbeitet und genutzt, die im Zusammenhang mit ihrer Tätigkeit stehen.

Besucher des Vereinsgeländes oder von Vereinsveranstaltungen

Zur Gewährleistung der Sicherheit und/oder zu Zwecken der Gefahrenabwehr sowie der Strafverfolgung wird das Vereinsgelände videoüberwacht. Entsprechende Aufnahmen bleiben unter Verschluss, dienen bei Eintritt von Straftaten oder Rechtsverletzungen als Beweismittel und werden den Ordnungs- und/oder Strafverfolgungsbehörden zur Verfügung gestellt.
Eine Stadionordnung regelt den Umgang mit der Videoüberwachung. Jeder Besucher willigt unwiderruflich sowie zeitlich unbefristet für jegliche audiovisuellen Medien in die unentgeltliche Verwertung von Bild und/oder Ton seiner Person - insbesondere für Live-Übertragungen, Sendungen und/oder Aufzeichnungen - ein, die im Zusammenhang mit einer Veranstaltung, dem Trainingsbetrieb oder zu Zwecken der Gefahrenabwehr sowie der Strafverfolgung erstellt werden.

Gremienarbeit und Vereinsverwaltung

Sitzungsprotokolle von Gremien und Versammlungen werden nicht veröffentlicht. Sitzungsprotokolle von Mitgliedsversammlungen können beim Vereinsvorstand eingesehen werden.

§ 2

Daten werden an Dritte übermittelt

Verbände

Zu Verbänden (Landessportbund, Landesfachverband im Landessportbund NRW, Stadtsportbund und Fußball-Verband Mittelrhein) werden Mitgliedsdaten, Ergebnisse (z. B. Torschützen) und besondere Ereignisse (z. B. Platzverweise) übermittelt.

Der Verein hat keinen Einfluss auf die Nutzung und Weitergabe der übermittelten personenbezogenen Daten durch die Verbände.

Öffentlichkeitsarbeit

Im Rahmen der Öffentlichkeitsarbeit werden in Telemedien (z. B. indehahn.de, fupa.net, fussball.de, facebook.com, twitter.com) und/oder gegenüber Dritten (z. B. Presse) besondere Ereignisse des Vereinslebens (z.B. die Durchführung, Ergebnisse und Detailinformationen zu Spielen/Veranstaltungen oder die Hintergründe zu Feierlichkeiten/Vereinsarbeit) in unterschiedlicher Art und Weise (schriftlich, mündlich, bildlich, etc.) bekannt gemacht.

Name, Kontaktdaten und ausgeübte Funktion von Funktionsträgern des Vereins werden in Telemedien und Publikationen des Vereins veröffentlicht.

Internetkameras veröffentlichen ununterbrochen gering aufgelöste Bilder vom Sportplatz am Kitzenhausweg auf indehahn.de. Die Bilder der letzten 3 Tage sind jederzeit im Zeitraffer und als Einzelbilder abrufbar. Die Stadionkameras zeigen eine Übersicht des Geländes.

Einwände gegen Veröffentlichung

Ein Betroffener kann jederzeit gegenüber dem Vorstand Einwände gegen eine Veröffentlichung seiner Daten vorbringen. In diesem Fall unterbleibt in Bezug auf diesen Betroffenen eine weitere Veröffentlichung. Davon ausgeschlossen ist die Berichterstattung bei Ligaspielen und Turnieren (Ergebnisse und Ereignisse).

Werbemaßnahmen

Der Verein übermittelt keine personenbezogenen Mitgliedsdaten zu Werbezwecken an Dritte.

§ 3

Verpflichtung auf das Datengeheimnis ist obligatorisch

Personen, die mit der Verarbeitung von personenbezogenen Daten betraut sind, sind auf das Datengeheimnis zu verpflichten (siehe Anlage 1: Technische und organisatorische Maßnahmen zum Schutz von Daten sowie Anlage 2: Verpflichtung auf das Datengeheimnis).

§ 4

Mitglieder können Nutzung ihrer Daten freiwillig zustimmen

Ein gesunder Verein lebt auch von dem Austausch seiner Mitglieder untereinander. Deswegen ist es aus Sicht des Vereins wichtig, dass die Mitglieder miteinander leicht in Verbindung treten können. Dies wird durch die selektive Freigabe von personenbezogenen Daten innerhalb von einzelnen Abteilungen und Mannschaften unterstützt.
Entsprechende Regelungen zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten trifft der Mannschafts- oder Ressortverantwortliche direkt mit dem Betroffenen (zum Beispiel vor der Veröffentlichung von Spielerprofilen oder -informationen). Der Betroffene stimmt dem schriftlich zu.

§ 5

Bestellung eines Vereinsdatenschutzbeauftragten

Wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten befasst sind, ist durch den Verein ein Datenschutzbeauftragter zu bestellen. Der Datenschutzbeauftragte muss fachkundig, unabhängig und zuverlässig[1] sein. Er darf nicht zum Vorstand nach § 26 BGB gehören.

Aufgaben, Rechte und Pflichten des Datenschutzbeauftragten

Der Datenschutzbeauftragte des Vereins

- wirkt auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz hin,
- überwacht die ordnungsgemäße Anwendung der IT-Systeme, mit deren Hilfe personenbezogene Daten verarbeitet werden,
- schult die bei der Verarbeitung personenbezogener Daten tätigen Personen,
- kontrolliert automatisierte Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, vorab,
- stellt jedermann auf Antrag die Angaben über Verfahren automatisierter Verarbeitungen in geeigneter Weise zur Verfügung,
- überwacht alle notwendigen Maßnahmen im Falle einer Datenpanne nach §42a BDSG und
- geht Datenschutzbeschwerden von Betroffenen nach.

Der Datenschutzbeauftragte des Vereins hat die Pflicht, jeden ihm bekannten Verstoß gegen datenschutzrechtliche Anforderungen den Ressortleitern Vorsitz, IT und Verwaltung unverzüglich mitzuteilen. Der Vorstand hat daraufhin Maßnahmen zu ergreifen, um die Einhaltung datenschutzrechtlicher Anforderungen zu gewährleisten.

Jeder über diese Datenschutzordnung hinausgehende Umgang mit personenbezogenen Daten ist nur nach vorheriger Zustimmung durch den Vorstand und bei Notwendigkeit nach Einwilligung durch den Betroffenen oder seinen gesetzlichen Vertreter erlaubt.

[1] Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

§ 6

Grenzen des Datenschutzes durch den Verein

Der Austausch von Daten über Telemedien (Kurznachrichtendienste, Facebook, Twitter, Google+, Doodle, etc.) von Mitgliedern untereinander oder zwischen Mitgliedern und Funktionsträgern ohne Genehmigung durch den Vereinsvorstand ist rein privat. Insofern übernimmt der Verein für die nicht genehmigte Kommunikation untereinander keine Verantwortung.
Der Verein unterstützt die Mitglieder bei einer datenschutzkonformen Kommunikation zur Wahrung der informationellen Selbstbestimmung aller Betroffenen. Entsprechende Anfragen können an den Datenschutzbeauftragten gerichtet werden.

§ 7

Inkrafttreten

Die Datenschutzordnung tritt durch Beschluss des Vorstandes in Kraft.

Einstimmig beschlossen auf der Ressortleitersitzung am 20.05.2015

Dietmar Halterbeck
Ressortleiter Vorsitz

Anlagen

Anlage 1: Technische und organisatorische Maßnahmen zum Schutz von Daten

Die vereinseigenen, IT-technischen Systeme beschränken sich auf Überwachungskameras, einen Router mit Internetzugang und einen tragbaren PC zur Weitergabe von Spielergebnissen an den Fußball-Verband Mittelrhein.

Funktionsträger erheben, nutzen und verarbeiten personenbezogene Daten für den Verein über private IT-Systeme.

Zutrittskontrolle

IT-Systeme zur Erhebung, Nutzung und Verarbeitung von personenbezogenen Daten werden entweder im häuslichen Umfeld des Mitglieds/Funktionsträgers oder in der Geschäftsstelle des Vereins durch Verschluss (Sicherheitsschluss oder Schließanlage) gesichert.

Die Schließanlage der Geschäftsstelle gewährt nur denjenigen Personen Zutritt zu der Geschäftsstelle, die durch den Vorstand oder dessen Vertreter dazu ermächtigt wurde. Das Gebäude, in dem sich die Geschäftsstelle befindet, ist durch einen Zaun gesichert.

Zugangskontrolle

Alle IT-Systeme (häuslich und Geschäftsstelle) sind durch personenbezogene Kennungen zu sichern (Benutzername und Passwort).

Alle IT-Systeme (häuslich und Geschäftsstelle) sollten über die aktuellsten Sicherheitsupdates und einen aktuellen Virenschutz/Firewall verfügen.

Zugriffskontrolle

Es muss gewährleistet werden, dass die zur Benutzung von IT-Systemen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind, und dass personenbezogene Daten bei der Verarbeitung und Nutzung nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Alle IT-Systeme, auf denen sich personenbezogene Daten lokal befinden, werden durch einen Zugriffsschutz aus Benutzername und Kennwort geschützt.

Der Zugriff auf die Überwachungskameras des Vereinsgeländes ist passwortgeschützt. Damit erstellte Videoaufnahmen sind besonders vor Zugriff geschützt. Ausschließlich die Ressortvorstände Vorsitz und Informationstechnik haben Zugriff auf diese Aufnahmen. Veraltete (> 1 Monat) Aufnahmen werden laufend gelöscht.

Zur Erfüllung ihrer jeweiligen Aufgaben haben die folgenden Personen im dafür erforderlichen Umfang Zugriff auf die unter § 1 genannten personenbezogenen Daten:

a. Ressortvorstand Vorsitz, Verwaltung, Finanzen, Informationstechnik: Alle Belange
b. Weitere Ressortvorstände: Alle Belange betreffend das jeweilige Ressorts
c. Nachwuchs- und Jugendkoordinatoren: Alle Belange betreffend die Nachwuchsarbeit
d. Mannschaftsverantwortliche: Alle Belage betreffend die Mannschaft
e. Schiedsrichter, Presseverantwortlicher, Buchhalter, Mitgliedsverwalter, Sponsorenbetreuer, Webmaster, Revisoren, Datenschutzbeauftragter: Sonderaufgaben

Weitergabekontrolle

Es ist sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

E-Mail-Korrespondenz und elektronische Medien

Bei der vereinsinternen E-Mail-Kommunikation mit mehreren Mitgliedern oder der externen Kommunikation mit mehreren Empfängern wird der BCC-Modus (Blindkopie) bevorzugt verwendet. Im BCC-Modus wird die E-Mail zwar an alle im BCC-Feld aufgeführten Empfängerinnen und Empfänger verschickt, wer die E-Mail erhält, kann aber die anderen Adressen nicht erkennen.
Abteilungsintern oder mannschaftsbezogen (z. B. Lauftreff, Fussballmannschaften) ist es sinnvoll, dass zur kurzfristigen Abstimmung von Fahrgemeinschaften, Trainingsteilnahme etc. die E-Mailadresse oder die Telefonnummer allen Empfänger sichtbar ist.
Der Versand von personenbezogenen Daten über elektronische Medien ist nur in dem Umfang zulässig, in dem die Betroffenen dies regelmäßig erwarten (z. B. Kuchenspenden, Dienstpläne, Mannschaftsaufstellung).
Die darüber hinausgehende Übermittlung von personenbezogenen Daten über elektronische Medien ist nicht zulässig. Dies schließt die Gremienarbeit mit ein.

Eingabekontrolle

IT-Systeme, auf denen personenbezogene Daten verarbeitet werden, werden mit individualisierten Kennungen genutzt. Entsprechend kann nachträglich überprüft werden ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

Auftragskontrolle

Werden personenbezogene Daten im Auftrag durch Dritte verarbeitet, geschieht dies unter Beachtung datenschutzrechtlicher und informationssicherheitstechnischer Grundsätze. Dritte werden im Rahmen der Beauftragung zur Einhaltung dieser Grundsätze verpflichtet.

Verfügbarkeitskontrolle

Personenbezogene Daten werden gegen zufällige Zerstörung oder Verlust durch ausreichende Datensicherungsmaßnahmen geschützt.

Auf der Geschäftsstelle liegen die Daten zentral auf einen Datenserver zur Verfügung. Der Datenbestand wird zumindest täglich (inkrementelle/differentielle Sicherung) und wöchentlich (Vollsicherung) gesichert. Monatlich wird eine vollständige Datensicherungskopie an einen anderen Ort verbracht und sicher gegen unbefugten Zugriff aufbewahrt.

Trennungsgebot

Der Zugriff auf personenbezogene Daten geschieht auf Basis des Need-to-know-Prinzip. Näheres regeln die Vorgaben zur Zugriffskontrolle.

FC INDE HAHN e.V.

Anlage 2: Verpflichtung auf das Datengeheimnis (§5 BDSG)

Frau/Herr

_____

wurde heute darüber informiert, dass es ihr/ihm untersagt ist, personenbezogene Daten unbefugt zu anderen als dem der jeweiligen Aufgabenerfüllung dienenden Zwecken zu verarbeiten, bekannt zu geben, Dritten zugänglich zu machen oder sonst zu nutzen (Datengeheimnis).

Sie/Er wurde auf die Wahrung dieses Datengeheimnisses verpflichtet.

Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

Verstöße gegen das Datengeheimnis können nach §§ 43 BDSG mit Bußgeld und nach § 44 BDSG mit Geld- oder Freiheitsstrafe geahndet werden. Eine Verletzung des Datengeheimnisses kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen.

_____ _____

Ort, Datum Unterschrift der verantwortlichen Stelle

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung sowie ein Merkblatt mit Erläuterungen und dem Text der §§ 5, 43 und 44 BDSG habe ich erhalten.

_____ _____

Ort, Datum Unterschrift des Verpflichteten

Anlage 3: Merkblatt zur Verpflichtung auf das Datengeheimnis

Das BDSG gilt für den Umgang mit personenbezogenen Daten bei nicht-öffentlichen Stellen dann, wenn die Daten unter Einsatz von Datenverarbeitungsanlagen oder nicht automatisierten Dateien (Karteien, Sammlungen gleicher Formulare) verarbeitet, genutzt oder dafür erhoben werden, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Im Anwendungsbereich des BDSG richtet sich die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nach der zentralen Vorschrift in § 4 Abs. 1 BDSG, die wie folgt lautet:

"Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."

Die darin verwendeten Begriffe sind in § 3 BDSG definiert:

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Erheben ist das Beschaffen von Daten über den Betroffenen.

Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

a) die Daten an den Dritten weitergegeben werden oder

b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

§ 5 BDSG – Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das

Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43 Absatz 2 BDSG – Bußgeldvorschriften

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Abs. 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Abs. 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Abs. 1 Satz 2, § 30a Abs. 3 Satz 3 oder § 40 Abs. 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

§ 44 BDSG – Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.