Datenschutzkonzept

für die

Sandhaiser Narrenclique „Schlappgosch-Rudscha Waggis“

Stand: 13.03.2021

Inhaltsverzeichnis

1. Zweckbestimmung

1.1 Regelungsgegenstand

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten stellt stets einen Eingriff in die verfassungsrechtlich geschützte Sphäre der Betroffenen dar. Die Bindung an Recht und Gesetz verpflichtet alle Mitglieder, den Schutz personenbezogener Daten als wichtige Aufgabe zu verstehen. Alle Mitglieder haben bei ihrer täglichen Arbeit darauf zu achten, nicht gegen datenschutzrechtliche Bestimmungen zu verstoßen.

Dieses Konzept regelt Eckpunkte und Abläufe sowie Verantwortlichkeiten für alle Mitglieder des Vereins in Bezug auf den Umgang mit personenbezogenen Daten (pbD).

Vereinsbezogenes Datenschutzkonzept, Datenschutz der genutzten online-Dienstprogramme (TINEON AG), Datenschutz der sozialen Medien (FACEBOOK, INSTAGRAM) sowie die persönlichen IT-Sicherheitsschutzkonzepte, wie zum Beispiel NORTON sind als ein zusammenwirkendes Schutzsystem zu verstehen. Die genannten Schutzkonzepte sind daher jeweils in engem Zusammenhang anzuwenden.

1.2 Zielsetzung des Datenschutzkonzeptes

Mit dem Datenschutzkonzept werden die nachstehenden Zwecke verfolgt:

- kontinuierliche Sicherstellung der Einhaltung der zum Schutz des Grundrechts auf informationelle Selbstbestimmung bestehenden datenschutzrechtlichen Vorgaben,
- Verdeutlichung und Optimierung des eingeführten Datenschutzmanagements und Verbesserung der bestehenden Datenschutzorganisation im Verein,
- Bildung eines Datenschutzbewusstseins bei allen Mitgliedern.

1.3 Beachtung des Datenschutzkonzeptes

Die Mitglieder des Vereins haben sich mit dem Datenschutzkonzept vertraut zu machen und seine Regelungen zu beachten und umzusetzen. Sie sind aufgerufen, durch Vor-

schläge an der Optimierung des Datenschutzsystems und der IT-Sicherheit mitzuwirken.

2. Rechtliche Grundlagen

2.1 Verfassungsrechtliche Grundlagen

Das in Artikel 1 Abs. 1 und Artikel 2 Abs. 1 Grundgesetz verankerte allgemeine Persönlichkeitsrecht enthält auch die Befugnis des/der Einzelnen, grundsätzlich selbst zu entscheiden, wann, innerhalb welcher Grenzen und wem gegenüber seine/ihre persönlichen Daten offenbart werden. Dieses Recht auf informationelle Selbstbestimmung ist seit dem „Volkszählungsurteil“ des Bundesverfassungsgerichts (15.12.1983) verfassungsrechtlich anerkanntes Schutzgut.

Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Die das überwiegende Allgemeininteresse bestimmenden Voraussetzungen sind gesetzlich in den nachstehenden bereichsspezifischen und allgemeinen datenschutzrechtlichen Bestimmungen geregelt.

2.2 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) ist die allgemeine, gesetzliche Grundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er/sie durch den Umgang mit seinen/ihren personenbezogenen Daten in seinem/ihrem Persönlichkeitsrecht unzulässig beeinträchtigt wird.

3. Grundsätze des Datenschutzes

3.1 Rechtmäßigkeit

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, wenn

- das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder
- die Einwilligung des/der Betroffenen vorliegt.

Das Vorhandensein einer dieser Voraussetzungen ist bei jedem Umgang mit personenbezogenen Daten zu prüfen. Ohne Rechtsgrundlage oder Einwilligung erhobene, verarbeitete oder genutzte Daten sind unverzüglich zu löschen.

3.2 Erforderlichkeit

Zur rechtmäßigen Aufgabenerfüllung muss die Kenntnis der personenbezogenen Daten dem Grunde nach erforderlich und die Erhebung, Verarbeitung und Nutzung jedes einzelnen personenbezogenen Datums notwendig sein.

Personenbezogene Daten dürfen nur zur Erfüllung solcher Aufgaben gespeichert und ge-nutzt werden, für die der Verein

- örtlich,
- sachlich und
- funktionell

zuständig ist.

Bei der Datenverarbeitung muss im Interesse der Betroffenen die Art und Weise der Verarbeitung so gewählt werden, dass das Recht auf informationelle Selbstbestimmung so wenig wie möglich beeinträchtigt wird. Die Verarbeitungsmöglichkeiten sind entsprechend zu beschränken. Bei der Verarbeitung ist nach den Grundsätzen der Datensparsamkeit (so wenig Daten wie möglich) bzw. der Datenvermeidung (keine Erhebung, soweit nicht erforderlich) vorzugehen.

Die Daten dürfen nur solange gespeichert werden, wie sie zur Aufgabenerfüllung gebraucht werden. Die Notwendigkeit der weiteren Speicherung ist daher in regelmäßigen Abständen zu prüfen.

3.3 Zweckbindung

Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet oder genutzt werden, zu dem sie erhoben wurden.

Ziel der Zweckbindung ist es, zu verhindern, dass durch willkürliches Sammeln und Verarbeiten von personenbezogenen Daten die betroffene Person „gläsern“ wird.

Deshalb ist der Grundsatz der Zweckbindung nicht nur bei der Übermittlung von Daten aus dem Verein heraus an Dritte, sondern auch bei der Weitergabe von Daten innerhalb des Vereins zu beachten.

Eine Zweckänderung - wie sie in der Regel bei der Datenübermittlung oder Datenweitergabe vorliegt - erfordert eine entsprechende Erlaubnisvorschrift oder die Einwilligung der betroffenen Person.

3.4 Transparenz

Der Umgang mit personenbezogenen Daten muss für die betroffene Person nachvollziehbar sein.

Darüber hinaus muss es möglich sein, die Art und Weise, mit der personenbezogene Daten erhoben, verarbeitet oder genutzt werden, nachzuvollziehen. Das setzt eine entsprechende Dokumentation voraus, die kontinuierlich fortzuschreiben ist. Diese Dokumentationen sind Ausgangspunkt für Kontrollen des/der Administrativen Datenschutzbeauftragten (ADSB).

Es ist also im Rahmen der technisch-organisatorischen Maßnahmen zu dokumentieren,

- wie und von welcher Stelle/Person die Daten in den Verein gelangt sind,
- an welche Stellen die Daten innerhalb des Vereins weitergegeben worden sind sowie
- an welche andere datenschutzrechtlich verantwortliche Stelle außerhalb des Vereins die Daten übermittelt worden sind (z.B. Empfangsbestätigung / Sendebericht fordern).

Dadurch wird die Grundlage geschaffen,

- ein Auskunftsersuchen der betroffenen Person beantworten zu können und
- der Pflicht entsprechen zu können, Stellen, die personenbezogene Daten erhalten haben, über die Unrichtigkeit dieser Daten zu unterrichten (Nachberichtigungspflicht).

3.5 Erheben, Verarbeiten, Nutzen

Es dürfen nur die personenbezogenen Daten erhoben werden, die zur Aufgabenerfüllung benötigt werden. Eine Datenerhebung auf Vorrat ist unzulässig. Personenbezogenen Daten sind grundsätzlich bei dem/der Betroffenen zu erheben. Ohne seine/ihre Mitwirkung dürfen sie nur erhoben werden, wenn

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
- die Art der zu erfüllenden Verwaltungsaufgabe dies erforderlich macht oder
- die Erhebung bei dem/der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde.

Bei der zweiten und dritten Variante sind die tragenden Erwägungen zu dokumentieren.

Das Speichern, Verändern und Nutzen personenbezogener Daten ist nur zulässig, wenn und solange es zur Aufgabenerfüllung erforderlich ist und für den gleichen Zweck erfolgt, zu dem diese Daten erhoben worden sind.

Personenbezogene Daten sind unverzüglich zu löschen bzw. zu vernichten, wenn sie zur Aufgabenerfüllung nicht mehr benötigt werden und keine entgegenstehenden Aufbewahrungs- bzw. Speicherfristen existieren.

3.6 Technisch-organisatorische Maßnahmen

3.6.1 Schutzziele

Bei der Aufgabenerfüllung des Vereins sind die in der nachstehenden Tabelle dargestellten Schutzziele zu berücksichtigen. Die Schutzziele sind technologieunabhängig definiert; sie bilden einen Sicherheitsrahmen, der auch bei neuen Formen der Datenverarbeitung gewährleistet werden muss.

Schutzziel	Definition
Vertraulichkeit	Nur Befugte dürfen personenbezogene Daten zur Kenntnis nehmen.
Integrität	Personenbezogene Daten bleiben während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei.
Verfügbarkeit	Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden.
Authentizität	Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden.
Revisionsfähigkeit	Es kann jederzeit festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
Transparenz	Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig, aktuell und in der Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen
	werden können.
Wahrung der Rechte betroffener Personen	Die betroffene Person muss in der Lage sein, in einem gewissen Rahmen selbst auf den Umgang mit ihren personenbezogenen Daten einzuwirken.

3.6.2 Schutzbedarf

Gemäß § 9 BDSG ergibt sich aus der Art der personenbezogenen Daten deren Schutzbedarf. Dabei unterscheidet man zwischen den allgemeinen Arten personenbezogener Daten und den besonderen Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG.

- Zu den allgemeinen Arten personenbezogener Daten zählen alle personenbezogenen Daten, die nicht den besonderen Arten personenbezogener Daten im Sinne des §3 Abs. 9 BDSG zuzuordnen sind. Dies sind die Funktionsträgerdaten und alle übrigen personenbezogene Daten allgemeiner Art.

- Funktionsträgerdaten sind Daten, die für die Gestaltung des Vereinsbetriebes notwendig sind und nur für diese Zwecke verwendet werden. Dies sind nachfolgend abschließend aufgeführte Identifikationsdaten:

    - Name und Vorname,
    - Funktion und Tätigkeitsbereich,
    - private Haus-, Post- und E-Mail-Adresse,
    - private Telefon- und Faxnummer.

- Diese Daten haben einen geringeren Schutzbedarf als die übrigen personenbezogenen Daten allgemeiner Art. Personenbezogene Daten mit geringem Schutzbedarf werden dem **Schutzbereich 1** zugeordnet.

- Alle übrigen personenbezogenen Daten allgemeiner Art haben i.d.R. einen mittleren Schutzbedarf und sind grundsätzlich dem **Schutzbereich 2** zuzuordnen.

- Ausgenommen sind allgemeine Arten personenbezogener Daten, die in hohem Maße schutzwürdig sind. Solche Daten sind dem **Schutzbereich 3** zuzuordnen**.**

§ 3 Abs. 9 BDSG

- Besondere Arten personenbezogenen Daten sind gemäß § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung (z.B. Konfession), Gewerkschaftszugehörigkeit, Gesundheit (z.B. Tauglichkeits- und Verwendungsgrad, Grad der Behinderung) oder Sexualleben (z.B. eingetragene Lebenspartnerschaft). Diese Daten sind in hohem Maße schutzbedürftig. Personenbezogene Daten mit hohem Schutzbedarf sind dem **Schutzbereich 3** zuzuordnen.

3.7 Datenpflege

Personenbezogene Daten unterliegen der Veränderung und sind daher routinemäßig und anlassbezogen auf ihre Richtigkeit zu überprüfen und ggf. zu berichtigen.

3.8 Datensicherung

Personenbezogene Daten müssen zur Aufgabenerfüllung jederzeit kurzfristig verfügbar sein. Daher sind die zur Datensicherung notwendigen Maßnahmen in einem Datensicherungskonzept festzulegen und entsprechend durchzuführen.

3.9 Kontrollen

Die Beachtung der gesetzlichen Bestimmungen beim Umgang mit personenbezogenen Daten wird von unterschiedlichen internen und externen Stellen kontrolliert.

3.10 Rechte der Betroffenen

3.10.1 Unterrichtung/Benachrichtigung

Im Regelfall ist der/die Betroffene bei der Datenerhebung über

- die Identität der verantwortlichen Stelle,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorie von Empfängern, an die Daten übermittelt bzw. weitergegeben werden,

zu unterrichten. Die Unterrichtung umfasst auch Angaben über die Speicherdauer und eine evtl. Übermittlung an andere Stellen.

Erfolgt die Datenerhebung nicht bei der betroffenen Person, so ist diese grundsätzlich in entsprechender Weise zu benachrichtigen.

3.10.2 Auskunft

Der/Die Betroffene hat ein Recht auf Auskunft über

- die zu seiner/ihrer Person gespeicherten Daten,
- deren Herkunft,
- die Empfänger der personenbezogenen Daten innerhalb und außerhalb des Vereins sowie
- den Zweck ihrer Speicherung

3.10.3 Berichtigung/Nachberichtigung

Die Speicherung unrichtiger Daten beeinträchtigt die schutzwürdigen Interessen des/der Betroffenen. Diese Beeinträchtigung liegt in der Speicherung und der daraus folgenden ständigen Gefahr einer Übermittlung oder Nutzung unrichtiger Daten. Der/Die Betroffene hat Anspruch auf Beseitigung dieser dauernden Beeinträchtigung schutzwürdiger Interessen. Die Berichtigung ist unverzüglich entweder durch Veränderung oder durch Löschung durchzuführen.

3.10.4 Löschung/Sperrung

Daten sind zu löschen, wenn ihre Speicherung unzulässig war oder die Kenntnis der Daten für die speichernde Stelle zur Aufgabenerfüllung nicht oder nicht mehr erforderlich ist. Unzulässig ist die Speicherung von Daten, die nicht zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist. Die Löschung kann sich auf ein einzelnes Datum oder auf alle Daten des/der Betroffenen beziehen.

An die Stelle der Löschung tritt eine Sperrung, soweit

- einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
- Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des/der Betroffenen beeinträchtigt würden, oder
  hältnismäßig hohem Aufwand möglich ist. Bei der Beurteilung ist der Aufwand für die Löschung (finanzielle und technische Mittel, Personal- und Zeitaufwand) mit den schutzwürdigen Interessen der betroffenen Person an der Löschung ihrer personenbezogenen Daten abzuwägen. Die Gründe sind in einem Vermerk festzuhalten.

Ein Recht auf Sperrung personenbezogener Daten besteht ferner, wenn deren Richtigkeit von der/dem Betroffenen bestritten wird, und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

3.10.5 Widerspruch

Der/Die Betroffene kann einer automatisierten Erhebung, Verarbeitung und Nutzung seiner/ihrer personenbezogenen Daten widersprechen, wenn sein/ihr schutzwürdiges Interesse wegen der besonderen persönlichen Situation das Interesse der verantwortlichen Stelle überwiegt. Dies gilt jedoch nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

3.10.6 Weitere Rechte

Der/Die Betroffene hat ferner aus dem Umgang mit seinen/ihren personenbezogenen Daten folgende Rechte:

- Recht, sich an den Vereinsvorstand zu wenden, wenn er/sie der Ansicht ist, bei der Verarbeitung der personenbezogenen Daten in seinen/ihren Rechten verletzt zu sein
- Recht auf Folgenbeseitigung
- Recht auf Schadenersatz
- Recht auf Beantragung der Einleitung eines Bußgeldverfahrens
- Recht auf Stellung eines Strafantrages.

4. Verantwortungsbereiche

Der nachstehende Datenschutz-Organisationsplan legt die Verantwortlichkeiten und Aufgaben der genannten Funktionsträger des Vereins in datenschutzrechtlichen Angelegenheiten verbindlich fest. Die Datenschutzaufgaben werden integriert wahrgenommen; sie sind in den Geschäftsverteilungsplan aufzunehmen.

Verantwortlich für die Vollständigkeit und die Fortschreibung des Datenschutz-Organisationsplans ist der Vereinsvorstand.

4.1 Vereinsbezogene Datenschutzorganisation

4.1.1 Der Vorstand

Der Vorstand ist Adressat derjenigen Normen des BDSG, die dem Verein in seiner Funktion als verantwortliche Stelle näher bestimmte Verantwortlichkeiten, Befugnisse und Aufgaben zuweisen. Er/Sie trägt die Gesamtverantwortung für den Schutz der personenbezogen Daten, die der Verein zur Wahrnehmung zugewiesener Aufgaben für sich selbst erhebt, verarbeitet oder nutzt oder dies durch Dritte oder andere im Auftrag vornehmen lässt.

Bei der Erfüllung seiner/ihrer datenschutzrechtlichen Aufgaben wird der Vorstand durch weitere Funktionsträger bei Bedarf unterstützt.

Der 1. Vorstand, in Abwesenheit dieser der 2. Vorstand, ist auch für die Durchführung und Überwachung aller Maßnahmen der IT-Sicherheit im Verein verantwortlich.

4.1.2 Mitglieder des Vereins

Alle Mitglieder sind beim Umgang mit personenbezogenen Daten für die Beachtung der gesetzlichen sowie vereinsinternen Bestimmungen und Vorgaben selbst verantwortlich. Sie haben sich ständig mit den einschlägigen Regelungen insbesondere im eigenen Fachgebiet vertraut zu machen und diese umzusetzen. Die allgemeinen datenschutzrechtlichen Regelungen werden über die Homepage des Vereins im Mitgliederbereich verfügbar gehalten.

4.2 Administrativer Datenschutz

Zur Wahrnehmung der datenschutzrechtlichen Aufgaben im Rahmen der Fachaufsicht nach § 18 BDSG wurde im Verein der Administrative Datenschutz institutionalisiert.

4.2.1 Administrative/-r Datenschutzbeauftragte/-r

Die Funktion des/der ADSB wird in Zusammenhang mit einer Fachaufgabe aus dem Vorstand wahrgenommen. Diese Funktion greift erst, wenn mehr als 10 Mitglieder mit personenbezogenen Daten innerhalb des Vereins arbeiten.

Das Aufgabengebiet des administrativen Datenschutzes umfasst im Wesentlichen

- die Beratung und Unterstützung des Vorstandes in Angelegenheiten des Datenschutzes,
- das Koordinieren der Datenschutzmaßnahmen innerhalb des Vereins,
- die Prüfung der Zulässigkeit der rechtmäßigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in Dateien,
- die Erarbeitung von Antwortschreiben auf Beschwerden, Anträge u.ä., wenn datenschutzrechtliche Belange berührt sind,
- die Kontrolle der Verfahren und Einhaltung der Rechtsgrundlagen sowie der Zweckbestimmung,
- die Unterrichtung der Mitglieder im Verein in Angelegenheiten des Datenschutzes,
- die Erstellung von Hilfsmitteln zur Aufgabenwahrnehmung nach dem BDSG,
- die Vorbereitung und Begleitung von Kontrollen durch BfDI sowie die Koordinierung und Erarbeitung von Stellungnahmen zu Prüfberichten dieser Kontrollinstitutionen.

Der/Die ADSB unterliegt der Verschwiegenheitspflicht hinsichtlich der Identität betroffener Personen.

Zur Wahrnehmung der Aufgaben ist der/die ADSB befugt, auch unangemeldet fachaufsichtliche Prüfungen sowie Kontrollen zur Einhaltung des Datenschutzes im Verein einschließlich in den dezentralen Anteilen durchzuführen. Hiervon ist allerdings nur in geringem Umfang insbesondere in begründeten Fällen Gebrauch zu machen.

Fachaufsichtliche Prüfungen sind ansonsten grundsätzlich als Unterstützung in Bezug auf die rechtmäßige Durchführung der von der geprüften Organisationseinheit wahrzunehmenden Aufgaben zu verstehen. Daher sind sie in der Regel in Zusammenarbeit mit den zu prüfenden Stellen des Vereins zu planen und ggf. in Verbindung mit datenschutzrechtlichen Schulungen durchzuführen.

Durch fachaufsichtliche Prüfungen soll frühzeitig vereinsinterner Handlungsbedarf erkannt werden. Das Ergebnis der Prüfung wird durch den/die ADSB ausgewertet und ggf. so aufbereitet, dass sie als Datenschutzhinweis auf die Webseite eingestellt werden können.

Die Prüfkompetenz der/des ADSB umfasst

- die Durchführung angekündigter oder unangekündigter Kontrollen der Rechtmäßigkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in automatisierten Verarbeitungen,
- die Durchführung von Kontrollen zur Einhaltung der Weisungen des Vereins bei Verarbeitung oder Nutzung personenbezogener Daten im Auftrag oder durch Dritte,
- das Einsichtsrecht in alle personenbezogenen Daten im gesamten Verein.

Die Prüfkompetenz ist nur zum Schutz personenbezogener Daten zu nutzen. Die durch Prüfungen gewonnenen Informationen sind zu keinem anderen Zweck zu verwenden. Eine Leistungskontrolle findet im Rahmen der von dem/der ADSB durchgeführten Prüfung nicht statt.

Bei der Ausübung der Prüfungskompetenz ist § 14 Abs. 4 BDSG zu beachten.

4.3 IT-Sicherheitsbeauftragter / IT-Sicherheitbeauftragte

Der/Die IT-Sicherheitsbeauftragte des Vereins, wird aus dem Vorstand bestimmt und ist zuständig für

- die Beratung der Leitung des Vereins,
- die Anwendung/Umsetzung der IT-Sicherheit, ggf.
  Erstellen von konkreten Handlungsanweisungen, soweit Besonderheiten des Verein dies fordern,
- die Erarbeitung und Fortschreibung des vereinsbezogenen IT-Sicherheitskonzeptes unter Berücksichtigung der im Verein privat betriebenen IT-Projekte/-Systeme,
- die Durchführung von Kontrollen zur Überwachung von Maßnahmen zur Herstellung und Gewährleistung der IT-Sicherheit im Verein;
- die Empfehlung zur Freigabe von IT-Systemen zur Sicherung der Daten,
- die Bearbeitung von IT-Sicherheitsverstößen,
- das Führen der IT-Sicherheitsdokumentation.

Handelt es sich bei den Nutzerdateien erkennbar um Dateien mit personenbezogenen Daten, ist zur Wahrung der datenschutzrechtlichen Belange die Zustimmung der von der Überprüfung betroffenen Person einzuholen.

Verweigert die betroffene Person die Einsichtnahme unter Hinweis auf datenschutzrechtliche Gründe, so hat der/die IT-SiBe die Möglichkeit, die Überprüfung dennoch durchzuführen, wenn der/die ADSB hinzugezogen wird. Der/Die ADSB prüft, ob die Datei personenbezogene Daten enthält. Weist die Datei keine personenbezogenen Daten auf, führt der/die IT-SiBe die Prüfung fort.

Enthält die Datei personenbezogene Daten, informiert der/die ADSB den/die IT-SiBe darüber, welchem Schutzbereich diese zuzuordnen sind

5. Verfahrens- und Prüfabläufe

5.1 Zentral vorgegebene Verfahren

Bei zentralen Vorhaben ist davon auszugehen, dass die anordnende Stelle die datenschutzrechtlich notwendigen Prüfschritte bereits durchgeführt hat.

Der/Die ADSB ist über die Nutzung solcher Vorhaben innerhalb des Vereins durch die Vorhabenverantwortlichen in Kenntnis zu setzen.

5.2 Verfahrens- und Prüfabläufe im Verein

5.2.1 Beteiligung des/der ADSB

Der/Die ADSB ist ständig bei allen Vorgängen und Vorhaben/Projekten zu beteiligen, die sich auf den Umgang mit personenbezogenen Daten beziehen.

5.2.2 Automatisierte Verarbeitungen

Automatisierte Verarbeitungen liegen vor, wenn der Umgang mit pbD mit Hilfe von Datenverarbeitungsanlagen erfolgt. Umgang umfasst die Erhebung, Verarbeitung und Nutzung von pbD. Datenverarbeitungsanlagen sind z.B. PCs, Laptops, u.ä.; nicht aber Geräte, die lediglich der Übertragung von Informationen dienen (Faxgeräte, Kopierer ohne Speichermöglichkeit, etc.).

Um die Einhaltung bereichsspezifischer und allgemeiner datenschutzrechtlicher Bestimmungen bereits bei der Planung sicherzustellen, sind automatisierte Verarbeitungen, die auf den Umgang mit personenbezogenen Daten zielen, frühzeitig und umfassend mit den Ansprechpartnern für datenschutzrechtliche Angelegenheiten des Vereins sowie dem/der ADSB zu erörtern.

Automatisierte Verarbeitungen von personenbezogenen Daten sowie alle Änderungen daran sind vor Nutzungsbeginn/-änderung dem/der ADSB zur datenschutzrechtlichen Mitprüfung vorzulegen.

Für datenschutzrechtliche Mitprüfungen durch den/die ADSB ist durch den Verein offen zu legen,

- auf welcher gesetzlichen Grundlage der Umgang mit personenbezogenen Daten erfolgt,
- welchem konkreten Zweck der Umgang mit den personenbezogenen Daten dient,
- ob der Umgang mit personenbezogenen Daten als solcher, aber auch jedes Merkmal (z.B. Name, Vorname), Geburtsort erforderlich ist,
- wie konkret Merkmale bezeichnet werden können (keine Merkmale: Bemerkungen, Sonstiges, etc.),
- wie lange die personenbezogenen Daten zur Wahrnehmung der konkreten Aufgabe gespeichert werden müssen und - welche - ggf. unterschiedlichen - Löschungsfristen festgelegt werden müssen,
- wer den Zugriff auf die personenbezogenen Daten benötigt,
- wer die personenbezogenen Daten innerhalb des Vereins für seine Aufgabenerfüllung unter Beachtung der Zweckbestimmung ebenfalls benötigt,
- wie die personenbezogenen Daten gepflegt werden sollen,
- welche technisch-organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten ergriffen werden,
- welche Auswertungen oder Abfragen zur Aufgabenerfüllung notwendig sind.

5.2.3 Übermittlung / Weitergabe von Daten

Die Übermittlung personenbezogener Daten an externe Stellen ist nur zulässig, wenn sie zur Aufgabenerfüllung entweder der absendenden oder empfangenden Stelle notwendig ist. Sollte mit der Datenübermittlung eine Zweckänderung verbunden sein, setzt dies eine entsprechende gesetzliche Grundlage oder Einwilligung voraus. Die Weitergabe personenbezogener Daten innerhalb des Vereins zur Nutzung zu anderen Zwecken ist an die gleichen Voraussetzungen gebunden.

Bei Ersuchen auf Datenübermittlung von öffentlichen und nicht-öffentlichen Stellen ist nach den Vorschriften der §§ 15 und 16 BDSG zu §§ 15, 16 BDSG zu verfahren. Der/Die ADSB ist dabei von Anfang an zu beteiligen.

6. Aus- und Fortbildung

Für alle Beteiligte Datenschutz ist eine auf den Verein ausgerichtete datenschutzrechtliche Aus- und Fortbildung vorzusehen.

Art und Intensität der Aus- und Fortbildung orientieren sich an der Sensitivität der personenbezogenen Daten, mit denen bei der Aufgabenwahrnehmung umgegangen wird.

Folgende Ausrichtungen kommen in Betracht:

- Aus- und Fortbildung von Mitgliedern aus dem Vorstand,
- Aus- und Fortbildung von Multiplikatoren,
- Fortbildung unter Ausrichtung auf bereichsspezifische datenschutzrechtliche Bestimmungen (SG, BBG, usw.).

Die Aus- und Fortbildung kann auch unter Nutzung ressortinterner oder externer Angebote erfolgen.

Eine datenschutzrechtliche Basisschulung jedes einzelnen Mitgliedes geschieht wie folgt:

- durch eine erste Orientierung mittels des bei Aufnahme in den Verein auszuteilenden Merkblattes zum Thema Datenschutz.

7.1 Bundesbeauftragte/-r für Datenschutz und Informationsfreiheit

Der/Die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI)[22] wird vom Deutschen Bundestag gewählt. Jedermann kann sich an den BfDI wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Die Eingaben sind zu richten an:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30

53117 Bonn

poststelle@bfdi.bund.de

8. Fortschreibung

Dieses Datenschutzkonzept ist bei Eintritt von sicherheitsgefährdenden Ereignissen und wesentlichen Veränderungen im Verein oder Erlass neuer Vorgaben zum Datenschutz fortzuschreiben. Unabhängig davon ist jährlich die Notwendigkeit einer Fortschreibung zu prüfen. Die Fortschreibung ist zu dokumentieren.