Verpflichtungserklärung

für Mitarbeiterinnen und Mitarbeiter sowie Funktionsträger der Schwimm- und Sportfreunde Bonn e.V.

Name / Abteilung des/der Beschäftigten:

Die datenschutzrechtlichen Vorschriften verlangen, dass Daten mit Personenbezug so verarbeitet werden, dass die Rechte und Freiheiten der durch die Datenverarbeitung betroffenen Personen gewährleistet werden. Wir als Sportverein legen großen Wert auf Vertraulichkeit und Integrität der uns anvertrauten Daten. Deshalb ist es Ihnen als Beschäftigte/r, Trainer/in bzw. Übungsleiter/in oder sonstiger Funktionsträger/in der SSF Bonn auch nur gestattet, personenbezogene Daten im zur Erfüllung Ihrer Aufgaben erforderlichen Umfang zu verarbeiten. Unter den Begriff der personenbezogenen Daten fallen alle Daten, die sich direkt oder indirekt (über zusätzliche Informationen) einem bestimmten Menschen zuordnen lassen. Zu personenbezogenen Daten zählen beispielsweise Name, Anschrift, Kontaktdaten, Geburtsdatum / -ort, Gesundheitsdaten, Bankverbindung oder auch Kfz-Kennzeichen; lediglich Daten ohne jeglichen Bezug zu natürlichen Personen fallen nicht unter diese Kategorie. Es ist die vereinsweite Vorgabe der SSF Bonn, dass in Zweifelsfällen davon ausgegangen werden soll, dass Daten personenbezogen sind.
Zentrale Vorschriften im Datenschutz sind in erster Linie die EU-Datenschutzgrundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG). Danach dürfen personenbezogene Daten nur verarbeitet werden, wenn die betroffene Person hierzu eingewilligt hat oder es eine Rechtsgrundlage gibt. Unter einer Verarbeitung wird jeder mit oder ohne Hilfe von EDV-Anlagen ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten verstanden, wie z.B. Erheben, Erfassen, Organisieren, Speichern, Verändern, Abfragen, Offenlegen, Löschen oder Vernichten.
Die Daten dürfen grundsätzlich nur zu den vorgesehenen Zwecken verwendet werden. Außerdem darf weder absichtlich noch unabsichtlich die Sicherheit der Datenverarbeitung verletzt werden, so dass es zu Veränderung, Vernichtung, Verlust der Daten oder zu Offenlegung bzw. Zugang durch unbefugte Dritte kommt.
Wenn Sie rund um das Thema Datenschutz Fragen haben oder sich unsicher sind, welche Regelungen zutreffen bzw. wie Sie sich verhalten sollen, können Sie sich jederzeit an die Geschäftsführung der SSF Bonn wenden. Außerdem steht Ihnen auch der Datenschutzbeauftragte der SSF Bonn unter der E-Mailadresse datenschutzbeauftragter@ssfbonn.de für Auskünfte zur Verfügung.
Verstöße gegen das Datenschutzrecht können von Seiten der Aufsichtsbehörden bzw. Gerichte – je nach Verstoß – mit einer Geldbuße von bis zu 20 Mio. Euro, einer Geldstrafe oder gar einer Freiheitsstrafe geahndet werden. Im Falle eines materiellen oder immateriellen Schadens kann die von der unzulässigen Datenverarbeitung betroffene Person darüber hinaus ggf. einen Schadensersatzanspruch geltend machen. Sollte der SSF Bonn durch Ihr datenschutzwidriges Verhalten ein Schaden durch Bußgelder oder Schadenersatzansprüche Dritter entstehen, führt dies ggf. zu Regressansprüchen Ihnen gegenüber. Ein Verstoß gegen Datenschutzvorschriften oder gegen diese Vertraulichkeitsverpflichtung stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.
Die Verpflichtung zur Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungsverhältnisses bzw. der Funktion, in der Sie für den Verein tätig sind, fort. Etwaige andere Vereinbarungen zwischen Ihnen und der SSF Bonn bleiben unberührt. Diese Vertraulichkeitsverpflichtung ersetzt jedoch eine unter Umständen zuvor erfolgte Verpflichtung auf das Datengeheimnis gem. § 5 BDSG-alt mit Wirkung zum 25.05.2018.
Bitte beachten Sie auch das im Anhang zu dieser Erklärung abgedruckte Merkblatt!

Hiermit verpflichte ich mich zur Einhaltung der o.a. Regelungen zur Vertraulichkeit. Eine Kopie dieser Erklärung inkl. Anhang ist mir ausgehändigt worden.

(Ort, Datum)	**(Unterschrift Beschäftigte/r)**

Anhang: Merkblatt zur Verpflichtungserklärung
(Stand: Mai 2018)

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen […] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).
Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen […] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).
Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.
Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
§ 42 BDSG
(1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.
(2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.
§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

Fernmeldegeheimnis

§ 88 TKG
(1) [1]Dem Fernmeldegeheimnis unterliegen der **Inhalt der Telekommunikation und ihre näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. [2]Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
(2) [1]Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. [2]Die Pflicht zur Geheimhaltung besteht **auch nach dem Ende der Tätigkeit** fort, durch die sie begründet worden ist.
(3) [1]Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. [2]Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. [3]Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. [4]Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. […]

Datenschutz
Informationen und Anweisungen für Verarbeiter von personenbezogenen Daten

Rechtsgrundlage
Der Schutz personenbezogener Daten ist als **Grundrecht** auf informationelle Selbstbestimmung nach dem deutschen Grundgesetz sowie als Primärrecht der EU anerkannt. Seit dem 25.05.2018 gilt EU-weit die **Datenschutz-Grundverordnung** (DSGVO). Aufgrund sog. Öffnungsklauseln gibt es auch ein neues Bundesdatenschutzgesetz (BDSG-neu), das aber nur in wenigen Punkten über die DSGVO hinaus für uns relevant ist. Für Landes- und kommunale Behörden gelten zudem zusätzlich deren Landesdatenschutzgesetze.

Definitionen
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder damit identifizierbare natürliche Person (Mitarbeiter, Mitglieder, Kunden, Lieferanten, Interessenten) beziehen, also Name, Adresse und sonstige Kontaktdaten, Alter, Geschlecht, Qualifizierung, Bilder etc.. Hierzu gehören aber auch **besonders sensible Daten**, deren Verarbeitung besonders strengen Bedingungen unterliegen. In diese Kategorie fallen insbes. Daten über rassische und ethnische Herkunft, politische, religiöse bzw. weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, biometrische sowie Gesundheitsdaten, Sexualleben und sexuelle Orientierung. Der Begriff „**Verarbeitung**“ umfasst die Erhebung/Beschaffung, Aufbewahrung/Speicherung, Verwendung/Nutzung, Veränderung, Weitergabe und Löschung von personenbezogenen Daten.

Grundsätze
Bezogen auf personenbezogene Daten ist zunächst alles verboten, was nicht ausdrücklich erlaubt wurde („**Verbot mit Erlaubnisvorbehalt**“). Die **rechtmäßige Verarbeitung** kann nur auf Grundlage einer Einzelerlaubnis/Einwilligung (zum Nachweis möglichst in schriftlicher Form!) oder durch sonstige Regelungen (Verträge, Gesetze, Verordnungen, Betriebsvereinbarungen, Satzungen etc.) erfolgen. Im Falle der **Einwilligung** gilt, dass diese **freiwillig** sein muss und **nur für den benannten Zweck** gilt.
Es gelten weiterhin die **Grundprinzipien** bei der Verarbeitung personenbezogener Daten:

- **Zweckbindung:** Verarbeitung nur für den vorgegebenen Zweck
- **Datensparsamkeit:** nur die für den vorgegebenen Zweck notwendigen Daten
- **Datensicherheit:** vor Verlust oder unberechtigter Weitergabe (Hierzu gehört auch die Anweisung, personenbezogene Daten, insbes. wenn sie sensibel oder umfassend sind, nicht mittels unverschlüsselter E-Mails zu verteilen sowie die Anweisung, dass E-Mail-Verteiler, soweit es sich nicht um rein interne Verteiler handelt - z. B. mittels Bcc:-Nutzung oder anderer technischer Möglichkeiten - von den Empfängern nicht auslesbar sein dürfen!)
- **Transparenz der Datenerhebung**: Direkterhebungsgrundsatz, d. h., i. d. R. Erhebung bei der betroffenen Person selbst
- **Löschgebot:** fällt der Zweck weg, fällt auch die Erlaubnis zur Datennutzung weg. Zu beachten sind hier allerdings etwaige steuer- und handelsrechtliche Aufbewahrungsfristen. Insbesondere nach dem Steuerrecht müssen Geschäftsbriefe (einerlei, ob in Papier oder elektronisch) auch nach Erledigung der „Geschäfte“ bis zum Ablauf der gesetzlichen Fristen aufbewahrt, d. h. archiviert werden. Diese archivierten Dokumente sind für jede weitere Verwendung - außer einer solchen der Finanzbehörden im Rahmen einer Betriebsprüfung - zu sperren. Beim Löschen elektronischer Dokumente muss auch daran gedacht werden den „Papierkorb“ zu löschen! Das „Löschen“ von Papierdokumenten darf nur mit einem DIN-gerechten Schredder oder mittels Beauftragung eines zertifizierten Entsorgers erfolgen!

Rechte der betroffenen Personen

- **Auskunftsrecht** über ihre von einer Institution gespeicherten Daten
- **Recht auf Berichtigung**, falls die Daten nicht (mehr) stimmen
- **Recht auf Löschung/“Vergessenwerden“**, aber nur, wenn dem nichts entgegensteht
- **Recht auf Einschränkung der Verarbeitung**

In diesem Zusammenhang besteht eine **Mitteilungspflicht an alle Empfänger personenbezogener Daten** über die Berichtigung, Löschung und Einschränkung der Verarbeitung. Aber **Achtung**: Die betroffenen Personen müssen zweifelsfrei identifiziert und die Berechtigung nachgewiesen sein! Hier ist immer der Vorgesetzten oder der DSB einzubeziehen, da dieser Vorgang entspr. **dokumentiert** werden muss!

Und wenn wirklich mal etwas passiert ist
Da sich die Bußgelder erheblich erhöht haben, müssen (auch nur mögliche) Datenpannen **unverzüglich** den Verantwortlichen (Vorstand/Geschäftsführer/Betriebsleiter) und dem Datenschutzbeauftragten gemeldet werden, damit diese fristgerecht entsprechend reagieren können!