Bund Deutscher
Schiedsmänner und Schiedsfrauen e. V. -BDS-
Bundesvereinigung

MEDIATION

Bund Deutscher Schiedsmänner und Schiedsfrauen e. V. - BDS -
Postfach 10 04 52 · 44704 Bochum

Datenschutzrichtlinie
Richtlinie für den Schutz von personenbezogenen Daten

1. Geltungsbereich
Diese Richtlinie gilt für alle Personen im Bund Deutscher Schiedsmänner und Schiedsfrauen e.V. - BDS – und dessen Untergliederungen (Angestellte und Ehrenamtliche), die Daten verarbeiten oder nutzen und für sämtliche personenbezogene Daten, die im BDS zur Durchführung der satzungsgemäßen Zwecke sowie damit im Zusammenhang stehenden Aufgaben verarbeitet oder genutzt werden. Darunter fallen alle Daten, unabhängig davon, ob die Daten automatisiert oder nicht automatisiert verarbeitet oder genutzt werden.
Diese Richtlinie kann durch besondere Anweisungen bzw. beim Einsatz spezieller Anwendungen ergänzt werden.

2. Zielsetzungen und Begriffsbestimmungen
Diese Richtlinie regelt den Umgang mit personenbezogenen Daten, die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten innerhalb des BDS.
Ziel dieser Richtlinie ist es, den Schutz und die Sicherheit personenbezogener Daten und Informationen sowie die Einhaltung von Datenschutzvorschriften zu gewährleisten.
Alle Zugriffsberechtigten haben geeignete und angemessene Vorkehrungen zu treffen, die eine ordnungsmäßige, störungsfreie, gegen Missbrauch, Verlust und Veränderung geschützte Informationsverarbeitung sowie den Schutz und die Sicherheit von Daten gewährleisten.

Datenschutzvorschriften regeln den Umgang mit personenbezogenen Daten.
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (= Betroffener), z.B.: Name, Vorname, Geburtstag, Adressdaten, E-Mail-Adresse, Telefonnummer.
Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Art und Umfang des Umgangs mit Daten des Einzelnen sind auf das erforderliche Maß zu begrenzen, um unverhältnismäßige Eingriffe in den privaten Lebensbereich zu verhindern (Schutz der Privatsphäre).

3. Beachtung von Rechtsvorschriften
Bei der Verarbeitung und Nutzung von Daten sind zu beachten:
- allgemeine Datenschutzvorschriften, insbesondere Bundesdatenschutzgesetz (BDSG)
- weitere besondere Rechtsvorschriften, soweit sie sich auf die Verarbeitung oder Nutzung von Daten beziehen (z.B. Steuerrecht, Arbeits- und Sozialrecht).

Verstöße gegen diese Richtlinie gelten als Pflichtverletzungen und können rechtliche Konsequenzen nach sich ziehen. Verstöße gegen Rechtsvorschriften können strafrechtlich verfolgt und gemäß den jeweiligen Strafvorschriften geahndet werden.

4. Einsatz der Informationstechnik (EDV)
Voraussetzungen für den Einsatz von Informationstechnik sind:
- die rechtliche Zulässigkeit der Informationsverarbeitung und deren Sicherungsmöglichkeit,
- die Information der Benutzer über Einsatzzweck sowie
- eine an den Zielen der Informationsverarbeitung orientierte Risikoanalyse und daraus abgeleitete Sicherheitsmaßnahmen.

5. Datensicherheit
Die Informationsverarbeitung und die Nutzung von personenbezogenen Daten sind bestimmten Risiken ausgesetzt.

Diese sind u.a. technisches Versagen, menschliches Fehlverhalten (Unkenntnis, Sorglosigkeit, Fahrlässigkeit, Vorsatz) oder höhere Gewalt.
Diesen Risiken muss mit Sicherheitsmaßnahmen, die auch Voraussetzung für die Umsetzung von Datenschutzbestimmungen sind, begegnet werden.
Hauptziele der Datensicherheit sind:
- Vertraulichkeit der Daten (keine unbefugte Kenntnisnahme),
- Integrität der Daten (keine Verfälschung),
- Verfügbarkeit der Daten (kein Verlust) und
- Verbindlichkeit (Zurechenbarkeit).

Sicherheitsmaßnahmen sind so auszuwählen, dass die beabsichtigte Schutzwirkung mit vertretbarem Aufwand erreicht wird und Einschränkungen in vertretbaren Grenzen bleiben.

Die gesetzlichen „Anforderungen an technische und organisatorische Maßnahmen der Datensicherheit“ ergeben sich aus der Anlage zu § 9 Satz 1 BDSG, welche dieser Richtlinie als **Anlage 1** beigefügt ist. Deren Umsetzung im BDS ist wie folgt geregelt:

Zutritt zu Technikräumen (Server, spezielle Archive mit Datentechnik usw.) haben nur die zuständigen Personen gemäß den Festlegungen im Arbeitsvertrag bzw. des Leiters der Bundesgeschäftsstelle. Diese Räume sind bei Abwesenheit grundsätzlich verschlossen zu halten.

Zugang zu Datenverarbeitungsanlagen und **Zugriff** auf konkrete Anwendungen und Daten haben nur die dazu berechtigten Personen. Das wird für das OnlineMitgliederVerzeichnis (OMV) durch eine entsprechende Beantragung und eine Anmeldeprozedur (Benutzername und Passwort) und unterschiedliche Zugriffsberechtigungen (Lese- und/oder Schreibberechtigung) geregelt.
Für Passwörter gilt:
- Das Passwort ist geheim zu halten.
- Bei Verdacht, dass das Passwort bekannt geworden ist, ist ein sofortiger Wechsel erforderlich.
- Keine Trivialpasswörter (z.B. nebeneinanderliegende Tasten, eigener Name), die leicht herauszufinden sind, benutzen.

Zugriffsrechte für das OMV sind durch die geschäftsführenden Vorstände der Landes- bzw. Bezirksvereinigungen schriftlich zu beantragen und werden vom IT-Beauftragten des BDS bzw. dessen Stellvertreter oder in deren Auftrag durch die Geschäftsstelle des BDS erteilt, geändert oder entzogen.
Zur Beantragung ist generell das entsprechende Formblatt zu verwenden.

Verpflichtung auf das Datengeheimnis: Jeder Zugriffsberechtigte sowie alle Mitarbeiter, die Umgang mit personenbezogenen Daten haben, werden bei der Aufnahme ihrer Tätigkeit bzw. bei der Erteilung der Zugriffsberechtigung schriftlich auf das Datengeheimnis (gemäß § 5 BDSG) und die Einhaltung dieser Richtlinie verpflichtet. Das Muster der „Verpflichtung auf das Datengeheimnis“ ist dieser Richtlinie als **Anlage 2** beigefügt. Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Datenträger jeglicher Art sind so aufzubewahren, dass sie nicht unbefugt gelesen, kopiert, verändert, gelöscht oder entfernt werden können.
Die Entsorgung von Datenträgern hat so zu erfolgen, dass Dritte keinesfalls Kenntnis vom Inhalt der Datenträger erhalten.

Alle Eingaben in das OMV werden zu Kontroll- und Nachweiszwecken automatisch protokolliert.

Zur Sicherstellung der **Verfügbarkeit** der Daten werden die Daten der Server regelmäßig gesichert.

6. Regeln zur Einhaltung des Datenschutzes
Es gelten die folgenden Grundsätze für das Erheben, Verarbeiten und Nutzen personenbezogener Daten im BDS, um dies in rechtlich zulässiger Art und Weise zu vollziehen.

Erheben, Speichern, Verändern und Übermitteln von Daten
Daten sind nur insoweit zu erheben, zu speichern, zu verändern und zu übermitteln wie dies für satzungsgemäße und vereinsinterne Zwecke erforderlich ist.
Es sind separate Festlegungen sowie gesetzliche Maßgaben zu beachten.
Unbefugtes Erheben, Speichern, Verändern und Übermitteln von Daten verstößt gegen Datenschutzvorschriften und andere Rechtsvorschriften und ist untersagt.
Die unzulässige Bekanntgabe/Weitergabe von Daten an Dritte ist verboten und zu verhindern.

Auskunft an den Betroffenen
Gemäß den geltenden Datenschutzbestimmungen und anderen Rechtsvorschriften hat der Betroffene das Recht auf Auskunft über seine personenbezogenen Daten.
Auskünfte über Daten Dritter werden grundsätzlich nicht erteilt, es sei denn, der Anfragende weist konkret nach, aus welchem Grund und zu welchem Zweck er Anspruch auf Auskunft hat. Vor jeder Auskunftserteilung im gesetzlichen Rahmen sind die Identität und Berechtigung des Anfragenden feststellen (keine Daten an Unbefugte herausgeben) sowie der Anfragende aufzufordern, näher zu bezeichnen, welche konkrete Information benötigt wird (Beschränkung auf erforderliche Daten).
Eine Auskunft an unberechtigte Dritte ist eine unzulässige Datenübermittlung.

Berichtigung von Daten
Unrichtige Daten sind umgehend zu berichtigen.

Löschung von Daten
Daten, deren Speicherung unzulässig ist, sind zu löschen. Daten, deren weitere Speicherung nicht mehr erforderlich ist, sind zu löschen, soweit diese nicht aufbewahrungspflichtig sind.
Um ungewollte oder unbefugte Löschung zu verhindern, sind Datenträger entsprechend zu schützen und Daten entsprechend zu sichern (Datensicherheit).

7. Verfahrensverzeichnis
Zur Schaffung von Transparenz innerhalb des BDS aber auch gegenüber Betroffenen wird das als **Anlage 3** dieser Richtlinie beigefügte öffentliche Verfahrensverzeichnis regelmäßig aktualisiert.
Bei Einführung neuer Verfahren oder Prozesse wird jeweils geprüft und beurteilt, ob diese besondere datenschutzrechtliche Risiken aufweisen, um entsprechende Festlegungen zu treffen.

8. Datenschutzbeauftragter
Der BDS hat nach Maßgabe der §§ 4f und d BDSG einen Datenschutzbeauftragten bestellt.
Dessen Kontaktdaten sind dem Verfahrensverzeichnis (Anlage 3) zu entnehmen bzw. im Internet unter www.schiedsamt.de veröffentlicht.
Der Datenschutzbeauftragte kontrolliert die Einhaltung von Datenschutzvorschriften und nimmt die ihm kraft Gesetzes sowie in dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr.
Bei Feststellung von Datenschutzverstößen ist der Datenschutzbeauftragte zu informieren.
Jedes BDS-Mitglied und jeder Mitarbeiter sowie sonstige Betroffene können sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den Datenschutzbeauftragten wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

9. Schlussbestimmung
Diese Richtlinie gilt ab 01. Februar 2018.

Anlagen:
Anlage 1 - Anforderungen an technische und organisatorische Maßnahmen der Datensicherheit
Anlage 2 - Verpflichtung auf das Datengeheimnis
Anlage 3 – Verfahrensverzeichnis