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

Datenschutzrichtlinie
Richtlinie zum Schutz von personenbezogenen Daten

1. Geltungsbereich
Diese Richtlinie gilt für alle Personen im BDS (Angestellte und Ehrenamtliche), die personenbezogene 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 personenbezogenen 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
Diese Richtlinie regelt den Umgang mit personenbezogenen Daten, die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten innerhalb des BDS.
Jede Person hat das Recht auf informationelle Selbstbestimmung. Das Speichern und Verarbeiten von personenbezogenen Daten sind daher nur in den gesetzlich vorgesehenen Fällen bzw. darüber hinaus mit Zustimmung des Betroffenen zulässig.

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 Datenverarbeitung sowie den Schutz und die Sicherheit der personenbezogenen Daten gewährleisten.

3. Beachtung von Rechtsvorschriften
Bei der Verarbeitung und Nutzung von Daten sind zu beachten:
- allgemeine Datenschutzvorschriften, insbesondere die EU-Datenschutz-Grundverordnung (EU-DSGVO), das Bundesdatenschutzgesetz (BDSG) sowie das jeweilige Landesrecht
- 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.

3. Begriffsbestimmungen
Datenschutzvorschriften regeln den Umgang mit personenbezogenen Daten.
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).

Personenbezogene Daten sind alle Informationen und Merkmale, die sich auf eine natürliche Person (= Betroffene/r) beziehen oder zumindest beziehbar sind und somit Rückschlüsse auf deren Persönlichkeit ermöglichen. Dazu gehören u.a. Name, Vorname, Geburtsdatum, Geschlecht, Adressdaten, E-Mail-Adresse, Telefonnummer, Personalausweisnummer, Kontonummer, Standortdaten, IP-Adresse.

Verarbeitung umfasst jeden - mit oder ohne automatisiertes Verfahren - ausgeführten Vorgang 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, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

4. Grundsätze der Datenverarbeitung

Die folgenden Grundsätze sind bei der Verarbeitung von personenbezogenen Daten zu beachten.

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Das heißt, Daten dürfen nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Alle Informationen zur Verarbeitung von personenbezogenen Daten sind leicht zugänglich sowie verständlich in einfacher und klarer Sprache abzufassen.

b) Zweckbindung

Dies bedeutet, dass Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Separat geregelt ist eine Weiterverarbeitung der erhobenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

c) Datenminimierung

Demnach dürfen Daten vom Umfang her nur dem Zweck angemessen und soweit erheblich erhoben werden und müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Insbesondere durch technische Voreinstellungen ist sicherzustellen, dass grundsätzlich nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den konkreten Zweck erforderlich ist.

d) Richtigkeit

Dementsprechend müssen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

e) Speicherbegrenzung

Dies bedeutet, dass Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Speicherfristen sind auf das unbedingt erforderliche Mindestmaß zu beschränken. Unter besonderen Bedingungen (vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen) dürfen personenbezogene Daten länger gespeichert werden, soweit diese ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden.

f) Integrität und Vertraulichkeit

Das heißt, dass Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung und unbeabsichtigter Schädigung.

5. Datensicherheit und Risikoanalyse

Die Verarbeitung von personenbezogenen Daten ist bestimmten Risiken ausgesetzt. Insbesondere kommen technisches Versagen, menschliches Fehlverhalten (Unkenntnis, Sorglosigkeit, Fahrlässigkeit, Vorsatz) oder höhere Gewalt in Betracht.
Diesen Risiken muss mit angemessenen Sicherheitsmaßnahmen begegnet werden.
In regelmäßigen Abständen ist eine Risikoanalyse durchzuführen und daraus müssen die konkret erforderlichen Sicherheitsmaßnahmen abgeleitet und umgesetzt werden.
Sicherheitsmaßnahmen sind so auszuwählen, dass die beabsichtigte Schutzwirkung mit vertretbarem Aufwand erreicht wird und Einschränkungen in vertretbaren Grenzen bleiben.

Bei Einführung neuer Verfahren zur Datenverarbeitung bzw. bei Verwendung neuer Technologien, welche voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben können, ist vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchzuführen. Diese **Datenschutz-Folgenabschätzung** erfolgt in Abstimmung mit dem Datenschutzbeauftragten.

Zur Sicherstellung der Datensicherheit sind die entsprechenden technischen und organisatorischen Maßnahmen durchzuführen bzw. einzuhalten.
Eine Übersicht zu den jeweils angewandten „**technischen und organisatorischen Maßnahmen** der Datensicherheit" liegt vor und wird laufend auf Aktualität überprüft. Wesentliche Schwerpunkte der Umsetzung im BDS sind wie folgt geregelt:

Zutritt zu Technikräumen (Server, speziellen Archive mit Datentechnik usw.) haben nur die zuständigen Personen. 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 die OnlineMitgliederVerwaltung (OMV) durch eine entsprechende Beantragung und eine Anmeldeprozedur (Benutzername und Passwort) und unterschiedliche Zugriffsberechtigungen (Lese- und/oder Schreibberechtigung) geregelt.
Für Passwörter gilt:
- Ein Passwort soll mindestens acht Zeichen umfassen.
- Es soll groß und klein geschriebene Buchstaben sowie Nummern und Sonderzeichen enthalten.
- Das Passwort ist geheim zu halten.
- Es sollen keine Trivialpasswörter (z.B. nebeneinanderliegende Tasten, eigener Name), die leicht herauszufinden sind, benutzt werden.

Zugriffsrechte für die OMV sind durch die Landes- bzw. Bezirksvorsitzenden schriftlich zu beantragen und werden vom IT-Beauftragten des BDS bzw. dessen Stellvertreter 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 und die Einhaltung dieser Richtlinie verpflichtet. Hierfür ist generell das erstellte Muster zu verwenden. 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 folgende Vorgaben 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 sowie gegebenenfalls andere Rechtsvorschriften und ist damit untersagt.
Die unzulässige Bekanntgabe bzw. Weitergabe von Daten an Dritte sind zu verhindern.

Auskunft an den Betroffenen bzw. Dritte
Gemäß den geltenden Datenschutzbestimmungen hat der Betroffene das Recht auf Auskunft über seine personenbezogenen Daten.
Daneben gibt es Auskunftsrechte auch nach anderen Rechtsvorschriften.

Auskünfte über Daten Dritter werden grundsätzlich nicht erteilt, es sei denn, der Anfragende weist konkret nach, aus welchem Grund (Benennung der Rechtsgrundlage) und zu welchem Zweck er einen Anspruch auf Auskunft hat.

Bei Auskunftsanfragen ist zu beachten:
- Die Identität und Berechtigung des Anfragenden sind feststellen (keine Auskunft an Unbefugte),
- Den Anfragenden auffordern, näher zu bezeichnen, welche Auskunft benötigt wird (eigenes Auskunftsrecht bzw. Beschränkung auf erforderliche Daten).
- Es ist zu prüfen, ob die Auskunft über bestimmte Angaben gegebenenfalls zu verweigern ist.

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 unverzüglich 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).

Meldepflicht bei Datenpannen
Wurde die Sicherheit personenbezogener Daten verletzt, z.B. durch Verlust oder unbefugte Offenlegung (Verlust von Datenträgern, Missbrauch von Passwörtern etc.), ist sofort die Geschäftsstelle des BDS zu informieren. Diese meldet den Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich (binnen 72 Stunden) nachdem die Verletzung bekannt wurde an die zuständige Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Die Information zur Datenpanne muss eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (Angabe der Kategorien der Daten und der ungefähren Zahl der betroffenen Personen), die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen enthalten.
Alle Datenpannen sind zu dokumentieren.

7. Verzeichnis von Verarbeitungstätigkeiten
Zur Schaffung von Transparenz innerhalb des BDS aber auch zur Erfüllung von Auskunftspflichten gegenüber Aufsichtsbehörden und Betroffenen werden alle Verarbeitungstätigkeiten bezüglicher personenbezogener Daten erfasst. Diese werden gemäß den gesetzlichen Vorgaben in dem „Verzeichnis von Verarbeitungstätigkeiten“ zusammengefasst. Das Verzeichnis wird regelmäßig auf Aktualität überprüft und gegebenenfalls entsprechend angepasst.
Bei Veränderungen bzw. Einführung neuer Verfahren oder Prozesse im Umgang mit personenbezogenen Daten ist die Geschäftsstelle des BDS umgehend zu informieren. Es wird jeweils geprüft und beurteilt, ob sich hieraus besondere datenschutzrechtliche Risiken ergebenen, um entsprechende Festlegungen bzw. Maßnahmen zu treffen.

8. Datenschutzbeauftragter
Der BDS hat nach Maßgabe der gesetzlichen Bestimmungen einen Datenschutzbeauftragten bestellt.
Dessen Kontaktdaten sind im Internet unter www.schiedsamt.de veröffentlicht.

Der Datenschutzbeauftragte unterrichtet über datenschutzrechtliche Vorschriften und berät hinsichtlich der Pflichten bei der Verarbeitung von personenbezogenen Daten. Er überwacht die Einhaltung von Datenschutzvorschriften sowie der Strategien zum Schutz personenbezogener Daten, sensibilisiert und schult die an den Verarbeitungsvorgängen beteiligten Personen und der diesbezüglichen Überprüfungen. Auf Anfrage berät der Datenschutzbeauftragte im Zusammenhang mit der Datenschutz-Folgenabschätzung. Weiterhin fungiert er als Anlaufstelle für die Aufsichtsbehörde und arbeitete mit dieser zusammen.
Der Datenschutzbeauftragte nimmt die ihm kraft Gesetzes zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr.
Bei Feststellung von Datenschutzverstößen ist der Datenschutzbeauftragte zu informieren.
Jedes BDS-Mitglied, jeder BDS-Mitarbeiter und jeder Betroffene kann 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. Januar 2019.