BERICHT 2023 DES DATENSCHUTZBEAUFTRAGTEN

Externer Datenschutzbeauftragter der NADA 2023: Dr. Ralf Schadowski

1. Zusammenfassung

Hiermit bescheinige ich als externer bestellter Datenschutzbeauftragter der Nationalen Anti Doping Agentur Deutschland (NADA) ein vorhandenes Datenschutz-Managementsystem gemäß Anforderung durch das gültige Bundesdatenschutzgesetz und der europäischen Datenschutz Grundverordnung (EU-DSGVO / GDPR).

Die NADA hat sich einer Aufnahme auf Basis BSI Grundschutz unterzogen, und hat die Handlungsempfehlungen umgesetzt. Insbesondere die nachstehenden Bereiche werden im Geltungsbereich des Datenschutzmanagement-Systems (DSMS) umgesetzt:

- Auftragsverarbeitung nach Art. 28 DSGVO
- Verfahrensverzeichnisse nach Art. 30 DSGVO
- Sachgerechtes Auskunftsverfahren nach Art. 15 DSGVO
- Technisch organisatorische Maßnahmen nach Art. 32 DSGVO
- Vertragsprüfung eingehender Verträge im Kontext Datenschutz
- Mitarbeitersensibilisierung

Das DSMS ist ein strukturiertes und systematisches Rahmenwerk / eine Methodik, welche die NADA dabei unterstützt, den Datenschutz in ihren Geschäftsprozessen und Aktivitäten zu verwalten, zu überwachen und zu verbessern. Ein DSMS ist darauf ausgerichtet, die Datenschutzanforderungen und -verpflichtungen einer Organisation zu erfüllen, insbesondere in Bezug auf die Datenschutzgesetze und -vorschriften.

Die Implementierung eines DSMS trägt dazu bei, Datenschutzrisiken zu minimieren, den Schutz personenbezogener Daten zu gewährleisten und das Vertrauen von Athlet*innen, Partner*innen, Mitarbeiter*innen und weiteren Stakeholdern in Bezug auf den Umgang mit ihren Daten zu stärken. Ein DSMS umfasst folgende Hauptkomponenten (Kritikalität 1), siehe Abbildung rechts.

Das DSMS liegt im Datenraum bei ADDAG im Rechenzentrum dauerhaft für die NADA bereit. Dort sind alle Dokumente, Richtlinien, Auftragsverarbeitungen nach Art. 28 DSGVO, Verfahrensverzeichnisse nach Art. 30 DSGVO, etc. gespeichert. Die NADA hat Zugriff und informiert den Datenschutzbeauftragten bei Änderungen (Prozesse, Vertragspartner, Technik, Tools, etc.). Der Reifegrad der Datenschutzanforderungen bei der NADA ist hoch und entspricht den Anforderungen. Wichtige Bereiche sind nachfolgend kurz erläutert.

2. Status Quo

2.1 Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO ist mit derzeit 30 beschriebenen Verfahren / Tätigkeiten aktuell für die Bereiche:

- Ressort Doping-Kontroll-System (DKS)
- Stabstelle Kommunikation
- Ressort Medizin
- Ressort Prävention
- Ressort Recht
- Verwaltung: Personalwirtschaft, IT Support

Neue Verfahren werden dem Datenschutzbeauftragten gemeldet und mit dem zuständigen Fachbereich der NADA dokumentiert. Vorhandene Verarbeitungstätigkeiten werden fortlaufend im Verzeichnis gepflegt. Die letzte Sichtung des Verzeichnisses der Verarbeitungstätigkeiten wurde am 14.03.2024 durchgeführt.

2.2 Erfüllung von Informationspflichten

Die Datenschutzhinweise für Webseiten und Portale wurden den Anforderungen entsprechend angepasst und im Falle einer Webseitenerneuerung durch Webseiten Checks ergänzend überprüft. Bei jeglichen Ansprachen wird stets die Umsetzung eines Einwilligungsprozesses bzw. das Vorliegen einer Rechtsgrundlage beachtet.

2.3 Umgang mit Datenlöschungen

Daten werden nach Wegfall der Rechtsgrundlage oder Widerruf der Einwilligung gelöscht oder gesperrt, je nach technischer Möglichkeit. Löschungsvorgaben gehen aus dem Verzeichnis der Verarbeitungstätigkeiten hervor. Die Umsetzung der Löschungen ist organisiert. Die Dokumentation der Organisation in einem Löschkonzept ist zu empfehlen und ist mit dem Datenschutzbeauftragten für das Jahr 2023 abzustimmen.

2.4 Betroffenenrechte

Das sachgerechte Auskunftsverfahren ist organisiert, die Datenspeicherorte und Ansprechpartner sind aufgrund der Verfahrensdokumentation identifiziert, der Prozess ist festgeschrieben und die Vorlage für etwaige

Darstellung des Datenschutz Managementsystem der NADA, Stand 31.12.2023

Nr. [lfd.]	Kritikalität [1-6]	Erfüllung [%]	Aufgabe (DSMS)
1	1	100	Benennung Datenschutzbeauftragte*r
2	1	100	Meldung DSB bei Aufsicht
3	1	93	**Auftragsverarbeitung nach Art. 28 DSGVO (AV)**
4	1	100	1. an Auftragnehmer, Freigabe Vorlage
5	1	100	1. an Partner (Auftragnehmer), Erstellung Vorlage
6	1	100	2. Erstellung Liste der Dienstleister (Kreditorencheck)
7	1	100	3. Versand der AV'en
8	1	100	4. Kontrolle Rückläufer
9	1	100	5. Abnahme der Rückläufer
10	1	100	6. Rückfragen der Dienstleister beantworten Stufe 1
11	1	100	7. Rückfragen der Dienstleister beantworten Stufe 2
12	1	80	von Auftraggeber, Prozess Freigabe
13	1	50	TOMs an Auftraggeber erstellen
14	1	n/a	**IC AV Verträge**
15	1	100	**Verfahrensverzeichnisse nach Art 30 DSGVO (VV)**
16	1	100	1. Einführungsworkshops, JEDE Fachabteilung
17	1	100	2. Erstellung 5-10 VV / Fachabteilung
18	1	100	3. Abnahme der VV
19	1	100	**Auskunftsverfahren an Betroffene nach Art. 15 DSGVO**
20	1	100	1. Gestaltung Prozess
21	1	100	2. Gestaltung Antwort Anschreiben
22	1	100	**Auskunft an Datenschutzaufsicht (72h)**
23	1	100	1. Gestaltung Prozess
24	1	100	2. Gestaltung Antwort Anschreiben
25	1	80	private EMAIL Nutzung regeln (VEWA)
26	1	90	Datenschutzhinweise Website Bewertung
27	1	70	EMAIL Bewerbungsprozess: Löschung nach Absage sicherstellen
28	1	50	Newsletter Einwilligungen sicherstellen
29	1	50	Datenschutz Information an Kunden (allgemein)
30	2	100	Mitarbeiter*innen VERPFLICHTUNGSERKLÄRUNG auf das Datengeheimnis
31	2	50	Löschkonzept bei Archivierung
32	2	90	Mitarbeiter*innensensibilisierung organisieren
33	2	25	Datenschutzkonzept
34	2	25	Datenschutzrichtlinie / Datenschutzleitlinie
35	2	100	NDA Vorlage festlegen
36	2	80	Datenschutz-Vorabkontrollen fehlen
37	2	10	Verschlüsselungsinventarisierung erstellen und bewerten
38	2	50	Einwilligungen Kunden Review, Unterlagen an Schadowski
39	3	50	Outsourcingrichtlinie (Haftung, Eigentumsrechte, Pönalen ...)
40	3	100	Liste der Abrufverfahren erstellen und bewerten
41	3	n/a	Video Richtlinie / Kennzeichnung der Videoüberwachung

Auskunftsersuchen wurde erstellt. Auskunftsersuchen werden sachgerecht in enger Zusammenarbeit mit dem Datenschutzbeauftragten beantwortet.

2.5 Datenschutzfolgenabschätzungen
Im Berichtszeitraum wurde eine Datenschutzfolgenabschätzung zur Softwarelösung Microsoft 365 durchgeführt. Die Maßnahmen zur Mitigation der Risiken wurden vom IT-Dienstleister schnell umgesetzt.

2.6 Datenschutzvorfälle
Im Berichtszeitraum kam es zu keinen meldepflichtigen Datenschutzvorfällen oder IT-Sicherheits-Störungen mit gravierenden Datenschutzfolgen für betroffene Personen. Alle Mitarbeitenden erreichen den Datenschutzbeauftragten direkt an 365 Tagen / 24h bei Datenschutz-Vorfällen zwecks Einhaltung der 72h Meldepflicht.

2.7 Auftragsverarbeitungsvereinbarungen
Alle relevanten Dienstleistende im Sinne der Auftragsverarbeitung nach Art. 28 DSGVO wurden vertraglich fixiert und stichprobenhaft geprüft. Eine Übersicht der eingesetzten Dienstleistende wurde tabellarisch erstellt. Die technischen und organisatorischen Maßnahmen sowie eingesetzte Unterauftragnehmer*innen wurden als Mindestgarantie geprüft und abgenommen.

3. Erteilte Datenschutz Sensibilisierungen
Die Mitarbeitenden werden regelmäßig auf den Datenschutz sensibilisiert. Die Teilnehmerlisten können bei Bedarf eingesehen werden. Die letzte Sensibilisierung fand am 28.03.2023 statt.

4. Änderungsmanagement
Der Datenschutzbeauftragte wird bei Bedarf angefordert, zum Beispiel bei:

- Erweiterungen / Änderung von IT Lösungen / IT-Infrastruktur
- Dienstleistende Verträgen (Neuanlage, Änderung)
- Prozess-Änderungen im Umgang mit personenbezogene Daten
- Datenschutz Anfragen von Auftraggebern / Dienstleistern
- Datenschutz Anfragen von Athlet*innen / Mitarbeiter*innen / sonstigen Betroffenen

5. Informationssicherheit
Die verantwortliche Stelle wurde einem BSI Grundschutzaudit unterzogen, Handlungsempfehlungen wurden umgesetzt. Im Berichtszeitraum kam es zu keinen wesentlichen IT-Störungen / Verletzungen der Informationssicherheit. Die NADA hat im Jahr 2023 ein ISMS aufgebaut, das die Datenschutz-Anforderung unterstützt.

6. Fortbildung und Fachkundenachweis
Der Datenschutzbeauftragte Dr. Ralf Schadowski ist externer Datenschutzbeauftragter des Verantwortlichen. Er ist persönlich ISO 17024 / 27701 zertifiziert im Bereich Datenschutz und damit fortlaufend überwacht. Er unterstützt die NADA mit 35 Datenschutz-Spezialist*innen aus seinem Team, die je nach Spezialist*innen ebenfalls aktuelle Ausbildungsstände aufweisen.

7. Sonstiges
Im Jahr 2024 werden die Maßnahmen zum Datenschutz bei der NADA fortgeführt. Insbesondere die (ggfs. digitalen) Mitarbeitersensibilisierungen sowie die notwendigen Review Arbeiten des DSMS sind in Planung. Weiterhin sind zu verschiedenen datenschutz- und IT-sicherheitstechnischen Dokumenten folgende Maßnahmen geplant:

- Review Datenschutzkonzept
- Review Datenschutzrichtlinie/ Datenschutzleitlinie
- Erstellung Kryptokonzept mit Verschlüsselungsinventarisierung
- Überarbeitung Löschkonzept

Direkter Kontakt bei Rückfragen zum ordentlich bestellten Datenschutzbeauftragten:

E-Mail: datenschutz@nada.de