BERICHT DES DATENSCHUTZBEAUFTRAGTEN

Externer Datenschutzbeauftragter der NADA ist Dr. Ralf Schadowski.

1. ZUSAMMENFASSUNG

1.1. Informationen zum ordentlich bestellten Datenschutzbeauftragten

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

Ich bestätige auch die Wahrung meiner Aufgaben als Datenschutzbeauftragter gemäß den Vorgaben nach Art. 39 DSGVO:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den Datenschutzvorschriften;
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeitenden und der diesbezüglichen Überprüfungen;
- Beratung, auf Anfrage, im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO;
- Zusammenarbeit mit der Aufsichtsbehörde und
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Die Nationale Anti Doping Agentur Deutschland 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 / §62 BDSG
- Verfahrensverzeichnisse nach Art 30 DSGVO / §70 BDSG
- Sachgerechtes Auskunftsverfahren nach Art 15 DSGVO / §34 BDSG
- Technisch organisatorische Maßnahmen nach Art 32 DSGVO / §64 BDSG
- Datenschutz Richtlinie
- Datenschutz Mitarbeiter*innen-sensibilisierung

1.2 Darstellung des Datenschutz Managementsystem der NADA, Stand 31.12.2022

Nr. [lfd.]	Kritikalität [1-6]	Erfüllung [%]	Aufgabe (DSMS)
1	1	100	Bestellung Datenschutzbeauftragter
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	75	**Verfahrensverzeichnisse nach Art 30 DSGVO (VV)**
16	1	100	1. Einführungsworkshops, JEDE Fachabteilung
17	1	75	2. Erstellung 5-10 VV / Fachabteilung
18	1	50	3. Abnahme der VV
19	1	88	**Auskunftsverfahren an Betroffene nach Art 15 DSGVO**
20	1	75	1. Gestaltung Prozess
21	1	100	2. Gestaltung Antwort Anschreiben
22	1	88	**Auskunft an Datenschutzaufsicht (72h)**
23	1	75	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	10	Löschkonzept bei Archivierung
32	2	90	Mitarbeiter*innensensibilisierung organisieren
33	2	19	Datenschutzkonzept
34	2	10	Datenschutzrichtlinie / Datenschutzleitlinie
35	2	100	NDA Vorlage festlegen
36	2	80	Datenschutz-Vorabkontrollen fehlen
37	2	10	Verschlüsselungsinventarisierung erstellen und bewerten
38	2	10	Einwilligungen Kunden Review, Unterlagen an Schadowski
39	3	10	Outsourcingrichtlinie (Haftung, Eigentumsrechte, Pönalen ...)
40	3	1	Liste der Abrufverfahren erstellen und bewerten
41	3	n/a	Video Richtlinie / Kennzeichnung der Videoüberwachung

2. STATUS QUO DES VERANTWORTLICHEN

Das Verzeichnis der Verarbeitungstätigkeiten führt Verfahrensverzeichnisse konform zur DSGVO Art. 30 in den Bereichen

- IT
- Verwaltung / Sekretariate
- Rechnungsabteilung
- Bürokommunikation / *Office* / Schreibabteilung

Weitere Verfahrensverzeichnisse sind in der Erstellung. Diesbezüglich gibt es ein Verzeichnis der Verarbeitungstätigkeiten, das dies umfasst.

Vorhandene Verfahrensverzeichnisse werden fortlaufend gepflegt.

Für 2023 muss der nächste Reviewprozess der dokumentierten Verfahrensverzeichnisse mit den jeweiligen Abteilungsverantwortlichen geplant und mit dem Datenschutzbeauftragten koordiniert und durchgeführt werden.

2.2 Erfüllung von Informationspflichten

Die Datenschutzhinweise für die Webseite werden den vorgegebenen gesetzlichen Anforderungen entsprechend aktualisiert und angepasst.

2.3 Datenlöschung

Personenbezogene Daten werden nach Wegfall der Rechtsgrundlage oder bei 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. Datenschutzkonzept (Art. 5 Abs. 2 DSGVO)

Das Datenschutzkonzept des Verantwortlichen hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

Der Schutz von personenbezogenen Daten hat für den Verantwortlichen einen hohen Stellenwert. Durch die DSGVO soll das Recht auf informationelle Selbstbestimmung geschützt werden. Dieses Grundrecht ist als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Dafür sind Regelungen zum Umgang mit den Daten nötig. Mit personenbezogenen Daten muss vertraulich umgegangen werden. Das Datenschutzkonzept hilft bei der Organisation und beim Vorgehen im Datenschutz. Mit den vorgegebenen Regelungen gewinnen die Mitarbeitenden Sicherheit im Umgang mit den personenbezogenen Daten. Sie sollen sich daran orientieren, es zeigt, welche Anforderungen einzuhalten sind. Das Datenschutzkonzept der NADA für das Jahr 2023 muss bis Ende Q2 2023 finalisiert werden.

2.5. Wahrung der Rechte der Betroffenen (Kapitel III DSGVO)

Das sachgerechte Auskunftsverfahren ist organisiert, die Datenspeicherorte und Ansprechpartner sind größtenteils identifiziert, der Prozess ist festgeschrieben und die Vorlage für etwaige Auskunftsersuchen wurde erstellt. Auskunftsersuchen werden weiterhin sachgerecht beantwortet.

2.6. Datenschutzvorfälle (Art. 33 DSGVO)

Im Berichtszeitraum vom 01.01.2022 bis 31.12.2022 kam es zu keinen meldepflichtigen Datenschutzvorfällen oder IT-Sicherheitsstörungen, die der zuständigen Aufsichtsbehörde gemeldet werden mussten. Der Eskalationsplan bei einem möglichen meldepflichtigen Datenschutzvorfall muss für das Jahr 2023 beim Verantwortlichen verschriftlicht werden.

2.7. Durchführung von Datenschutzsensibilisierungen (Art. 32 DSGVO)

Die Mitarbeitenden werden regelmäßig auf den Datenschutz sensibilisiert. Die zukünftigen Sensibilisierungen werden weiterhin beim Verantwortlichen vor Ort oder durch Videokonferenzen erfolgen.

2.8. Technische und organisatorische Maßnahmen (Art. 25 und 32 DSGVO)

Der Verantwortliche hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen technische und organisatorische Maßnahmen getroffen. Die vorliegenden Dokumentationen dieser getroffenen Maßnahmen sind ausreichend, da diese 2022 einem Review unterzogen wurden und ggf. dem Stand der Technik entsprechen.

2.9. Auftragsverarbeitungs-vereinbarungen

Alle relevanten Dienstleister im Sinne der Auftragsverarbeitung nach Art. 28 DSGVO wurden vertraglich fixiert und stichprobenhaft geprüft. Neue Auftragsverarbeiter werden dem Datenschutzbeauftragten vor Beauftragung gemeldet und von diesem geprüft.

2.10. Review der Datenschutzfolgenabschätzungen gemäß Art. 35 DSGVO

Für die folgend genannten Verfahren wurden im Jahr 2021 Datenschutzfolgenabschätzungen durchgeführt:

- ADAMS System
- RTS (*Remote Testing System*)

Hierbei wurden alle erkannten Risiken für betroffene Personen erfasst und anschließend festgestellt, dass die getroffenen Schutzmaßnahmen zu einer ausreichenden Mitigation der Risiken führen. Diese Risiken wurden anhand der Wahrscheinlichkeit des Auftretens und der Schwere der Auswirkungen bewertet. Aufgrund der getroffenen technischen und organisatorischen Maßnahmen mit ausführlicher Abwägungen der Datenschutzrisiken für die Persönlichkeitsrechte der Athleten und Athletinnen wurde ein akzeptables Restrisiko festgestellt.

Somit wurde auch nach Abschluss dieser Prüfung festgelegt, dass gemäß Art. 36 DSGVO keine vorherige Konsultation der Aufsichtsbehörde erfolgen musste und die Verfahren datenschutzkonform eingesetzt werden können. Diese Datenschutzfolgenabschätzungen müssen im Jahr 2023 in Abstimmung mit dem Datenschutzbeauftragten einem möglichen Review unterzogen werden.

2.11. Wesentliche Vorgänge des Datenschutzbeauftragten

Der Datenschutzbeauftragte wird bei Bedarf angefordert, zum Beispiel bei

- Erweiterungen der Infrastruktur
- Betrieb von IT-Lösungen
- Datenschutzanfragen von Athleten*innen
- Datenschutzanfragen von Mitarbeitenden
- Datenschutzanfragen von sonstigen Dritten
- ....

3. Fortbildung und Fachkundenachweis des Datenschutzbeauftragten

Der Datenschutzbeauftragte Dr. Ralf Schadowski ist externer Datenschutzbeauftragter des Verantwortlichen. Er ist persönlich ISO 17024 zertifiziert im Bereich Datenschutz und damit fortlaufend überwacht. Er unterstützt den Verantwortlichen mit 35 Datenschutz-Spezialisten aus seinem Team, die individuell ebenfalls aktuelle Ausbildungsstände aufweisen.

4. Aufgaben und Maßnahmen für das Berichtsjahr 2023

Im Jahr 2023 werden die Maßnahmen zum Datenschutz bei dem Verantwortlichen fortgeführt. Hierzu gehören die folgenden, aus dem Bericht zusammengefassten Aufgaben und Maßnahmen, die in diesem Jahr erfüllt und umgesetzt werden müssen:

- Review der Verzeichnisse der Verarbeitungstätigkeiten
- Review der Website und Anpassungen der Datenschutzerklärung
- Review und Aktualisierung des Prozesses des Sachgerechten Auskunftsverfahrens
- Fortwährende Prüfung neuer Software bzw. Verarbeitungstätigkeiten anhand von Datenschutzkurzpapieren/ DSFA
- Fortwährende Prüfung neuer Auftragsverarbeiter
- Fortwährende Aufnahme und Dokumentation von Datenschutzvorfällen
- Fortwährende Aufnahme und Dokumentation von Auskunfts- und Löschersuchen
- Durchführung und Überwachung von Datenschutzsensibilisierungen
- Finalisierung des Datenschutzkonzepts
- Abstimmung zur Dokumentation des Löschkonzepts
- Dokumentation des Eskalationsplans bei einem möglichen Datenschutzvorfall

Diese Aufgaben muss der Verantwortliche gemeinsam mit dem Datenschutzbeauftragten für das Jahr 2023 koordinieren und umsetzen, um seiner Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nachzukommen. Eine Nichterfüllung der Rechenschaftspflicht birgt ein hohes Risiko für das Verhängen von Bußgeldern durch die Aufsichtsbehörden gegenüber dem Verantwortlichen, deren Veröffentlichung auch einen hohen Imageverlust für eine Organisation wie die NADA zur Folge haben kann.

5. Abschluss des Datenschutzberichts für das Jahr 2022

Hiermit schließe ich meinen Bericht für das Jahr 2022 ab und stehe bei Rückfragen wie folgt zur Verfügung.

E-Mail: datenschutz@nada.de