

# REPORT 2023 OF THE DATA PROTECTION OFFICER

External Data Protection Officer of NADA 2023: Dr Ralf Schadowski

## 1. Summary

As the externally appointed data protection officer of the National Anti Doping Agency Germany, I hereby certify that a data protection management system is in place in accordance with the requirements of the applicable Federal Data Protection Act and the European General Data Protection Regulation (EU GDPR).

NADA Germany has undergone an audit based on BSI basic protection and has implemented the recommendations for action. In particular, the following areas are implemented within the scope of the data protection management system (DSMS):

- Order processing in accordance with Art. 28 GDPR
- Procedure directories in accordance with Art. 30 GDPR
- Appropriate information procedure in accordance with Art. 15 GDPR
- Technical and organisational measures in accordance with Art. 32 GDPR
- Contract review of incoming contracts in the context of data protection
- Employee sensitisation

The DSMS is a structured and systematic framework / methodology that helps NADA Germany to manage, monitor and improve data protection in its business processes and activities. A DSMS is designed to meet an organisation's data protection requirements and obligations, particularly in relation to data protection laws and regulations.

The implementation of a DSMS helps to minimise data protection risks, ensure the protection of personal data and strengthen the trust of athletes, part-

ners, employees and other stakeholders with regard to the handling of their data. A DSMS comprises the following main components (criticality 1), see figure on the right.

The DSMS is permanently available to NADA Germany in the data room at ADDAG's data centre. All documents, guidelines, order processing in accordance with Art. 28 GDPR, procedure directories in accordance with Art. 30 GDPR, etc. are stored there. NADA Germany has access and informs the data protection officer in the event of changes (processes, contractual partners, technology, tools, etc.). The maturity level of data protection requirements at NADA Germany is high and meets the requirements. Important areas are briefly explained below.

## 2. Status Quo

### 2.1 Register of processing activities

The register of processing activities in accordance with Art. 30 GDPR is currently complete with 30 procedures / activities described for the following areas:

- Testing Department (DKS)
- Communications Department
- Medicine Department
- Education Department
- Legal Matters
- Administration: Human Resources, IT Support

New procedures are reported to the data protection officer and documented with the responsible department at NADA Germany. Existing processing activities are continuously maintained in the register. The last review of the register of processing activities

was carried out on 14 March 2024.

### 2.2 Fulfilment of information obligations

The data protection notices for websites and portals have been adapted to the requirements and, in the event of a website renewal, additionally checked by website checks. The implementation of a consent process or the existence of a legal basis is always taken into account in any contact.

### 2.3 Dealing with data deletion

Data is erased or blocked after the legal basis ceases to apply or consent is withdrawn, depending on technical feasibility. Erasure requirements are set out in the record of processing activities. The implementation of deletions is organised. Documentation of the organisation in a deletion concept is recommended and must be agreed with the data protection officer for 2023.

### 2.4 Rights of data subjects

The appropriate information procedure has been organised, the data storage locations and contact persons have been identified on the basis of the procedural documentation, the process has been defined and the template for any requests for information has been created. Requests for information are answered appropriately in close cooperation with the data protection officer.

### 2.5 Data protection impact assessments

A data protection impact assessment was carried out for the Microsoft 365 software solution during the reporting period. The measures to mitiga-

## Description of NADA Germany's Data Protection Management System (DSMS), status 31.12.2023

No.	Criticality [1-6]	Compliance [%]	Task (DSMS)
1	1	100	Order of data protection officer
2	1	100	Notification of DSB to authority
3	1	93	<b>Order processing according to Art 28 DSGVO (AV)</b>
4	1	100	1. to contractor, release template
5	1	100	1. to partner (contractor), preparation of template
6	1	100	2. Preparation of the list of providers (creditor check)
7	1	100	3. Dispatch of the AV's
8	1	100	4. Controll returns
9	1	100	5. Decrease returns
10	1	100	6. Answer queries from providers Level 1
11	1	100	7. Answer queries from providers Level 2
12	1	80	from client, process release
13	1	50	create TOMs to client
14	1	n/a	<b>IC AV Contracts</b>
15	1	100	<b>Procedure directories according to Art 30 DSGVO (VV)</b>
16	1	100	1. Introductory workshops, EVERY department
17	1	100	2. Creation 5-10 VV / Department
18	1	100	3. Acceptance of the VV
19	1	100	<b>Information procedure to data subjects according to Art 15 DSGVO</b>
20	1	100	1. Design process
21	1	100	2. Design response cover letter
22	1	100	<b>Information to data protection authority (72h)</b>
23	1	100	1. Design process
24	1	100	2. Design response cover letter
25	1	80	regulate private EMAIL use (VEWA)
26	1	90	Privacy Policy Website Rating
27	1	70	EMAIL recruitment process: ensure deletion after rejection
28	1	50	Ensure newsletter consents
29	1	50	Data protection information to customers (general)
30	2	100	EMPLOYEES DECLARATION OF OBLIGATION to data secrecy
31	2	50	Deletion concept for archiving
32	2	90	Organise staff sensitisation
33	2	25	Data protection concept
34	2	25	Privacy Policy / Data Protection Guideline
35	2	100	Set NDA template
36	2	80	Lack of prior data protection checks
37	2	10	Create and evaluate encryption inventory
38	2	50	Consents Customer Review, Documents to Schadowski
39	3	50	Outsourcing policy (liability, property rights, penalties ...)
40	3	100	Create and evaluate the list of retrieval procedures
41	3	n/a	Video policy / marking of video surveillance

te the risks were quickly implemented by the IT service provider.

### **2.6 Data protection incidents**

In the reporting period, there were no reportable data protection incidents or IT security incidents with serious data protection consequences for data subjects. All employees can contact the data protection officer directly 365 days a year / 24 hours a day in the event of data protection incidents in order to comply with the 72-hour reporting obligation.

### **2.7 Order processing agreements**

All relevant service providers in terms of order processing in accordance with Art. 28 GDPR were contractually fixed and randomly checked. An overview of the service providers used was compiled in tabular form. The technical and organisational measures and subcontractors used were checked and approved as a minimum guarantee.

### **3. Data protection awareness training provided**

Employees are regularly sensitised to data protection. The lists of participants can be viewed on request. The last sensitisation took place on 28.03.2023.

### **4. Change Management**

The data protection officer is requested as required, for example in the event of:

- Extensions / changes to IT solutions / IT infrastructure
- Service provider contracts (new creation, changes)
- Process changes in the handling of personal data
- Data protection enquiries from clients / service providers
- Data protection enquiries from athletes / employees / other data subjects

### **5. Information Security**

The responsible organisation underwent a BSI basic protection audit and recommendations for action were implemented. There were no significant IT disruptions / breaches of information security during the reporting period. In 2023, NADA Germany established an ISMS that supports the data protection requirement.

### **6. Training and proof of expertise**

The data protection officer Dr Ralf Schadowski is the external data protection officer of the controller. He is personally ISO 17024 / 27701 certified in the area of data protection and is therefore continuously monitored. He supports NADA Germany with 35 data protection specialists from his team, who also have up-to-date training levels depending on the specialist.

### **7. Other**

The data protection measures at NADA Germany will be continued in 2024. In particular, the (possibly digital) employee sensitisation and the necessary review work of the DSMS are being planned. The following measures are also planned for various data protection and IT security documents:

- Review of data protection concept
- Review of data protection guideline/ data protection guideline
- Creation of crypto concept with encryption inventory
- Revision of deletion concept

Direct contact for queries to the duly appointed data protection officer:

E-mail: [datenschutz@nada.de](mailto:datenschutz@nada.de)

