DATA PROTECTION REPORT

Dr Ralf Schadowski is the responsible external data protection officer

1. SUMMARY

1.1. Information on the duly appointed data protection officer

Hereby I certify as the externally appointed data protection officer of the National Anti Doping Agency of Germany an existing data protection management system as required by the applicable Federal Data Protection Act and the European Data Protection Regulation (EU-DSGVO / GDPR).

I also confirm that I have fulfilled my duties as data protection officer in accordance with the requirements of according to Art. 39 DSGVO:

- Informing and advising the controller or processor and the employees who carry out processing operations, with regard to their obligations under the data protection regulations;
- Monitoring compliance with data protection rules as well as the controller's or processor's personal data protection policies, including assigning responsibilities, raising awareness and training employees involved in processing operations and carrying out checks in this regard;
- Advice, upon request, in relation to the data protection impact assessment and monitoring of its implementation in accordance with Art. 35 GDPR;
- Cooperation with the supervisory authority; and
- Acting as a point of contact for the supervisory authority on issues related to the processing, including prior consultation pursuant, to Art. 36 GDPR, and, where appropriate advice on all other issues.

The National Anti Doping Agency of Germany has undergone an admission on the basis of 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 according to Art 28 DSGVO / §62 BDSG
- Procedure directories according to Art 30 DSGVO / §70 BDSG
- Appropriate information procedure according to Art 15 DSGVO / §34 BDSG
- Technical organisational measures according to Art 32 DSGVO / §64 BDSG
- Data protection guideline
- Data protection employee sensitisation

1.2 Description of NADA Germany's Data Protection Management System, status 31.12.2022

No.	Criti-cality [1-6]	Compl-iance [%]	Task (DSMS Data Protection Management System)
1	1	100	Order of data protection officer
2	1	100	Notification of DSB to authority
3	1	93	**Order processing according to Art 28 DSGVO (AV)**
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	**IC AV Contracts**
15	1	75	**Procedure directories according to Art 30 DSGVO (VV)**
16	1	100	1. Introductory workshops, EVERY department
17	1	75	2. Creation 5-10 VV / Department
18	1	50	3. Acceptance of the VV
19	1	88	**Information procedure to data subjects according to Art 15 DSGVO**
20	1	75	1. Design process
21	1	100	2. Design response cover letter
22	1	88	**Information to data protection authority (72h)**
23	1	75	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	10	Deletion concept for archiving
32	2	90	Organise staff sensitisation
33	2	19	Data protection concept
34	2	10	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	10	Consents Customer Review, Documents to Schadowski
39	3	10	Outsourcing policy (liability, property rights, penalties ...)
40	3	1	Create and evaluate the list of retrieval procedures
41	3	n/a	Video policy / marking of video surveillance

2. STATUS QUO OF THE CONTROLLER

The directory of processing activities keeps procedural directories in conformity with DSGVO Art. 30 in the areas of

- IT
- Administration / Secretariat
- Accounting department
- Office communication / office / writing department

Further procedure directories are being compiled. In this respect, there is a directory of processing activities, that covers this.

Existing procedure directories are maintained on an ongoing basis.

For 2023, the next review process of the documented procedure directories must be planned with the respective department heads and coordinated and carried out with the Data Protection Officer.

2.2 Fulfilment of information obligations

The data protection information for the website is updated and adapted in accordance with the specified legal requirements.

2.3 Data deletion policy

Personal data will be deleted or blocked after the legal basis has ceased to exist or if consent is revoked, depending on technical feasibility. Deletion requirements are set out in the register of processing activities. The implementation of deletions is organised. The documentation of the organisation in a deletion concept is recommended and is to be coordinated with the Data Protection Officer for the year 2023.

2.4. Data protection concept (Art. 5 (2) GDPR)

The data protection concept of the controller aims to present the data protection aspects in a summarised documentation. It can also be used as a basis for data protection audits, e.g. by clients in the context of commissioned processing. This is not only to ensure compliance with the European General Data Protection Regulation (GDPR), but also to create evidence of compliance.

The protection of personal data is a high priority for the controller. The GDPR is intended to protect the right to informational self-determination. As a manifestation of the general right of personality under Article 2 (1) of the German Constitution in conjunction with Article 1 (1) of the German Constitution, this fundamental right is the right of the individual to determine for himself or herself the disclosure and use of his or her personal data. This requires regulations on the handling of data. Personal data must be handled confidentially. The data protection concept helps with the organisation and procedure of data protection. With the given regulations, the employees gain security in dealing with personal data. They should use it as a guideline; it shows which requirements must be met. NADA Germany's data protection concept for 2023 must be finalised by the end of Q2 2023.

2.5. Safeguarding the rights of data subjects (Chapter III GDPR)

The appropriate access procedure is organised, the data storage locations and contact persons have largely been identified, the process has been established and the template for any access requests has been drawn up. Requests for information continue to be answered appropriately.

2.6. 2.6 Data security incidents (Art. 33 DSGVO)

In the reporting period from 01.01.2022 to 31.12.2022, there were no reportable data security incidents or IT security incidents that had to be reported to the competent supervisory authority. The escalation plan in the event of a possible reportable data protection incident must be written down for the year 2023 at the controller.

2.7. Conduct data protection awareness training (Art. 32 GDPR)

Employees are regularly sensitised on data protection. Future awareness-raising sessions will continue to take place at the controller's premises or through video conferences.

2.8. Technical and organisational measures (Art. 25 and 32 GDPR)

The responsible person has implemented technical and organisational measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons. The existing documentation of these measures taken is sufficient, as these were subject to a review in 2022 and, where applicable, correspond to the state of the art.

2.9. Order processing agreements

All relevant service providers in terms of commissioned processing pursuant to Art. 28 of the GDPR were contractually fixed and randomly audited. New processors are notified to and reviewed by the Data Protection Officer prior to commissioning.

2.10. Review of the data protection impact assessments pursuant to Art. 35 of the GDPR

Data protection impact assessments were carried out in 2021 for the following procedures:

- ADAMS System
- RTS (Remote Testing System)

All identified risks for data subjects were recorded and it was subsequently determined that the protective measures taken lead to sufficient mitigation of the risks. These risks were assessed based on the probability of occurrence and the severity of the impact. Based on the technical and organisational measures taken, with detailed consideration of the data protection risks to the athletes' personal rights, an acceptable residual risk was determined.

Thus, even after completion of this assessment, it was determined that, pursuant to Art. 36 of the GDPR, no prior consultation of the supervisory authority had to take place and that the procedures could be used in a data protection-compliant manner. These data protection impact assessments must be subject to a possible review in 2023 in consultation with the data protection commissioner.

2.11. Prior data protection checks of essential processes

The Data Protection Officer will be requested as necessary, for example in the case of

- Extensions to the infrastructure
- operation of IT solutions
- data protection requests from athletes
- data protection enquiries from employees
- data protection requests from other third parties
- ....

3. Further training and certificate of competence of the data protection officer

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

4. Tasks and measures for the reporting year 2023

In 2023, the data protection measures will be continued at the data controller. This includes the following tasks and measures, summarised from the report, which must be fulfilled and implemented in this year:

- Review of the directories of processing activities
- Review of the website and adjustments to the privacy policy
- Review and update of the fair disclosure procedure process
- Ongoing review of new software or processing activities based on data protection briefs/DSFA
- Ongoing review of new processors
- Continuous recording and documentation of data protection incidents
- Continuous recording and documentation of requests for information and deletion
- Implementation and monitoring of data protection sensitisation
- Finalisation of the data protection concept
- Coordination of documentation of the deletion concept
- Documentation of the escalation plan in the event of a possible data protection incident

The controller must coordinate and implement these tasks together with the Data Protection Officer for 2023 in order to comply with its accountability obligation under Article 5(2) of the GDPR. Failure to comply with the accountability obligation carries a high risk of fines being imposed on the controller by the supervisory authorities, the publication of which may also result in a high loss of image for an organisation such as NADA Germany.

5. Conclusion of the data protection report for the year 2022

I hereby conclude my report for the year 2022 and am available for any queries as follows.

E-mail: datenschutz@nada.de