DATA PROTECTION REPORT

Dr. Ralf Schadowski is the responsible external data protection officer

1. Summary

Hereby I certify the existing data protection management system according to the requirements of the valid Federal Data Protection Act 2018 (new) and the General Data Protection Regulation (EU-DSGVO / GDPR) as an externally appointed data protection officer of the National Anti Doping Agency of Germany.

The National Anti Doping Agency of Germany has undergone an admission based on the BSI Basic Protection and has implemented the recommendations.

Specifically the following areas will be implemented in the DSMS data protection management system:

- Order processing according to Art 28 GDPR / §62 BDSG
- Procedural directories according to Art 30 GDPR / §70 BDSG
- Appropriate information procedure according to Art 15 GDPR / §34 BDSG
- Technical organizational measures according to Art 32 GDPR / §64 BDSG
- Privacy policy
- Data protection employee sensitization

2. Status Quo – Data Protection Management System

No	Criticality [1-6]	Compliance [%]	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

2.2 Procedure log
Up to this point, conform to DSGVO Art. 30 procedure directories have been created in the following areas:
- IT
- Administration / secretariat
- Accounting department
- Office communication / office / writing department

Further process directories are being created. Existing process directories are maintained continuously.

2.3 Fulfilment of information duties
The data protection information for websites and portals has been adapted to the requirements.

2.4 Data deletion policy
Data is deleted or blocked after the legal basis has ceased to exist or after a consent has been revoked, depending on the technical possibilities. Deletion instructions can also be found in the procedural indexes.

2.5 Rights of data subjects
The appropriate information procedure has been prepared, the process has been established and the template for possible requests for information has been drawn up.

2.6 Data security incidents
There were no reportable data protection incidents or IT security incidents in the reporting period. Attack attempts were made, which were always promptly reported to the data protection officer and logged.

2.7 Order processing agreements
All relevant service providers within the meaning of contract processing pursuant to Art. 28 GDPR were contractually fixed and randomly inspected.

2.8 Technical and organisational measures
The technical and organisational measures pursuant to Art. 32 of the GDPR were examined and approved as a minimum guarantee of compliance with the accountability obligations pursuant to Art. 5 of the GDPR.

2.9 Conducting data protection impact assessments pursuant to Art. 35 of the GDPR
During the reporting period, data protection impact assessments were carried out for the following two procedures:
- ADAMS System
- RTS (Remote Testing System)

In this process, 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, also after completion of this assessment, it was determined that, pursuant to Art. 36 of the GDPR, no prior consultation of the supervisory authority was required and that the procedures can be used in a data protection-compliant manner.

3. Providing training
The organisation's management highly values the annual data protection employee sensitisation (BDSG, TKG, EU GDPR) to comply with the accountability obligations pursuant to Art. 5 of the GDPR.

4. Prior data protection checks of essential processes
The data protection officer will be requested if necessary, for example: been created in the following areas:
- Infrastructure enhancements
- Operation of IT solutions
- Data protection requests from athletes
- Data protection requests from employees
- Data protection requests from other third parties
- ...

5. Information security
The responsible body was subjected to a BSI basic protection audit and recommendations were implemented. In the reporting period, there were no relevant IT disruptions, however a breach of information security took place which was immediately investigated and logged.

6. Training and evidence of specialist knowledge of the data protection officer
The data protection officer Dr Ralf Schadowski is the responsible external data protection officer. He is ISO 17024 certified in the area of data protec¬tion and is therefore continuously monitored. He supports the National Anti Doping Agency of Germany with his team of 37 data protection specialists, who also have the latest training levels depending on the specialist.

7. Other
The data protection work at the National Anti Doping Agency of Germany will continue in 2022.

Dr Ralf W. Schadowski
External Data Protection Officer