REPORT 2024 OF THE DATA PROTECTION OFFICER

External Data Protection Officer of NADA Germany 2024: Dr Bettina Kraft

Summary
The controller National Anti Doping Agency of Germany (NADA Germany), Heussallee 38, 53113 Bonn, operates a functioning data protection management system (DSMS), which implements the requirements of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act (BDSG). As part of an audit based on BSI basic protection / BDSG / GDPR, recommendations for action were defined, which were promptly implemented by the responsible party.

The following areas are maintained in the DSMS:

- Order processing in accordance with Art. 28 GDPR
- Records of processing activities in accordance with Art. 30 GDPR
- Appropriate information in accordance with Chapter III GDPR
- Technical and organisational measures in accordance with Art. 25, 32 GDPR
- Employee awareness training
- ...

The DSMS is a structured and systematic framework / methodology that supports NADA Germany in managing, monitoring and improving 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, partners, employees and other stakeholders with regard to the handling of their data.

The DSMS is permanently available to NADA Germany in the data room of SITS Deutschland GmbH in the data centre. All documents, guidelines, commissioned processing pursuant to Art. 28 GDPR, records of processing activities pursuant to 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.

Register of processing activities
The list of processing activities in accordance with Art. 30 GDPR is currently available with 30 procedures / activities described for the following areas

- Testing
- Communications & Marketing
- 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 19 March 2025.

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

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.

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.

Data protection impact assessments
During the reporting period, a data protection impact assessment was carried out for the expansion of the Microsoft 365 software solution. The measures to mitigate the risks were quickly implemented by the IT service provider.

Data protection incidents
During the reporting period, there were no reportable data protection incidents or IT security incidents with serious data protection consequences for data subjects. All employees contact the data protection officer in the event of data protection incidents in order to comply with the 72-hour reporting obligation.

Description of NADA Germany's Data Protection Management System (DSMS), status 31.12.2024

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	98	**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	100	create TOMs to client
14	1	100	**Procedure directories according to Art 30 DSGVO (VV)**
15	1	100	1. Introductory workshops, EVERY department
16	1	100	2. Creation 5-10 VV / Department
17	1	100	3. Acceptance of the VV
18	1	100	**Information procedure to data subjects according to Art 15 DSGVO**
19	1	100	1. Design process
20	1	100	2. Design response cover letter
21	1	100	**Information to data protection authority (72h)**
22	1	100	1. Design process
23	1	100	2. Design response cover letter
24	1	80	regulate private EMAIL use (VEWA)
25	1	90	Privacy Policy Website Rating
26	1	70	EMAIL recruitment process: ensure deletion after rejection
27	1	100	Ensure newsletter consents
28	1	100	Data protection information to customers (general)
29	1	100	EMPLOYEES DECLARATION OF OBLIGATION to data secrecy
30	2	100	Deletion concept for archiving
31	2	90	Organise staff sensitisation
32	2	100	Data protection concept
33	2	25	Privacy Policy / Data Protection Guideline
34	2	100	Set NDA template
35	2	100	Carrying out data protection impact assessments for potentially high-risk processing operations
36	2	10	Create and evaluate encryption inventory
37	2	100	Consents Customer Review
38	2	50	Outsourcing policy (liability, property rights, penalties ...)
39	3	100	Create and evaluate the list of retrieval procedures
40	3	n/a	Video policy / marking of video surveillance

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.

Data protection awareness training provided
Employees are regularly sensitised to data protection. The lists of participants can be viewed if required.

Topics/processes processed in the reporting period
- Appointment of Dr Kraft as external data protection officer
- Note on police operation/possible data protection incident
- Data protection audit - Shopify
- NADA Germany's TOMS in English
- Coordination on the planned use of new HR management software Personio
- Implementation of the data protection impact assessment M365 - PowerBI and Project
  o Coordination on handling requests from data subjects (surname)
  o Request for information from an athlete's contact person
  o Revocation of emails

Assessment of the current status and recommendations for next reporting period
The operation of the data protection management system is being continued intensively. One data protection incident was reported in the reporting period. This did not result in a report to the competent supervisory authority in accordance with Art. 35 GDPR. This initially indicates suitable and effective technical and organisational measures. This also shows that the reporting and notification processes at NADA Germany are working.

The direct involvement of the data protection officer in the processes on an ad hoc basis confirms the successful sensitisation of employees. The cooperation between the coordination team and the contact persons at SITS Deutschland GmbH works well.

The core element of a data protection management system is continuous improvement, for which measures already taken must be regularly checked for completeness and effectiveness.

In addition, new regulatory requirements and changes to the systems must be assessed and implemented. It is therefore important to provide with sufficient resources for regular tasks (such as planned jour fixes, DP audits, data subject enquiries, records of processing activities and possible data breaches) as well as for tasks that arise at short notice.

The following is therefore recommended for the coming reporting period
- Review and complete the processing directory including risk assessments
- On-site inspection to understand the local conditions and check the technical and organisational measures
- Conduct awareness-raising/training, in particular to support employees in the context of the DSMS, as these are also relevant to ISMS requirements
- Conduct emergency exercises (DS incident, IS incident, ransom ware attack, phishing attack)
- Check documents for completeness (e.g. consent, data protection information)

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

E-mail: datenschutz@nada.de