DNDi

Best Science
for the Most Neglected

DATA PROTECTION POLICY

Objective

This Data Protection Policy sets out DNDi's measures to ensure compliance with Data Protection law in respect to processing of Personal Data. The policy outlines high level principles while detailed instructions are captured in the relevant procedures and work instructions.

Any individual at DNDi, working at any of its offices and affiliated entities play an important role in ensuring that all Personal Data is handled according to the core principles described in this policy in order to guarantee the privacy and security of the Personal Data of our staff, clinical trials subjects, clinical trials staff, beneficiaries of DNDi treatments, partners, suppliers and others (as applicable).

This policy applies globally however, additional country-specific data protection requirements might apply and will be reflected in the local procedures, where applicable.

Scope

This policy is applicable to all Personal Data processing activities (including Personal Data made public by the Data Subject) for which DNDi is the Data Controller or Data Processor, regardless of the media on which that data is stored. Unless otherwise specified, the principles stated in this policy apply to both roles. This policy applies to all DNDi's staff, whose definition is available in Global Staff Policy.

The Swiss Federal Act on Data Protection (FADP) has been taken as basis for this policy. However, DNDi recognizes that, being established in different parts of the world and performing activities globally, any applicable Data Protection laws ought to be considered in case they set forth more stringent requirements. It is also acknowledged that laws other than Data Protection (e.g. laws on clinical trials) apply in addition to this policy.

Definitions

- **Data Controller**: natural or legal person who determines the purposes and means of processing Personal Data.
- **Data Processor**: natural or legal person who is responsible for processing Personal Data on behalf of a Data Controller.
- **Data Subject**: any living individual person directly or indirectly identifiable via Personal Data.
- **Data Protection Impact Assessment (DPIA)**: a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate, an assessment of the necessity and proportionality of the Processing in relation to its purpose, an assessment of the risk to the Data Subject and the risk mitigation measures in place and demonstration of compliance.
- **Data Protection Officer (DPO)**: a dedicated appointed role at DNDi responsible for supporting DNDi Staff with the implementation of this policy and interpretation of relevant Data Protection laws.
- **Data Protection Representative (DPR)**: The Data Protection Representative explicitly designated by a written mandate of DNDi to act on its behalf regarding its obligations if required under the applicable Data Protection laws.
- **DNDi Data Protection Network:** Representatives of DNDi's teams processing personal data who have regular contact with DNDi's DPO to identify required actions to improve Data Protection compliance within their functional areas (e.g. R&D, Communications, HR).

- **EU GDPR**: General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of Personal Data and on the free movement of such data.
- **Federal Act on Data Protection (FADP)**: legislation passed by the Swiss Parliament, updated in 2020 to ensure compatibility with EU GDPR and effective from September 1, 2023.
- **Personal Data**: any information relating to Data Subject, whether it relates to their private, professional, or public life. This data can be for example a name, photo, email address, bank details, medical information, IP address, social networks sites posts or a combination of the data that directly or indirectly identifies the person. Personal Data includes pseudonymised data which can be attributed to a Data Subject by the use of additional information (e.g. a code list) and/or the combination of data elements included in the dataset (e.g. location, age and disease); but excludes anonymous data or Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.
- **Personal Data Breach**: any act or omission that compromises the security, confidentiality, integrity, or availability of Personal Data or the physical, technical, administrative or organizational safeguards that DNDi or its third-party service providers put in place to protect it. The loss or unauthorized access of Personal Data is a Personal Data Breach.
- **Processing of data**: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Pseudonymised data**: personal data which have undergone the process of pseudonymisation, for example, replacing names or other identifiers with a reference number. The reference number can be tied back to the individual however it is held separately. Pseudonymisation is a security measure. .
- **Sensitive Personal Data**: information revealing racial or ethnic origin, political, trade-union, religious or philosophical views or activities, data on the intimate sphere, physical or mental health data, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning a natural person's sex life or sexual orientation, social security measures, administrative or criminal proceedings and sanctions.
- **UK GDPR:** means the GDPR, as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018, and as amended.

Policy

Principles of personal data processing

Processing of Personal Data at DNDi is oriented around the following principles:

- **Lawfulness, Fairness, Transparency and Proportionality:** DNDi will process Personal Data in a lawful, fair, and transparent manner, in good faith and in a proportionate manner. DNDi shall not process Personal Data if the Data Subject has expressly objected to the processing.

- **Purpose limitation:** DNDi will collect Personal Data for specific purposes that the Data Subject can recognize and will further process this Personal Data in a manner that is compatible with this purpose.

- **Storage limitation:** DNDi retains Personal Data no longer than necessary for the purpose for which they were processed, unless the public interest, scientific research or statistical purposes require a longer storage period. At the end of the retention period a review is carried out to determine whether the Personal Data is still required. Depending on the findings of the review, the retention period is extended, or the Personal Data are deleted or rendered permanently anonymous.
- **Accuracy:** Personal Data must be accurate and, where necessary, kept up to date. DNDi will take every reasonable step to ensure that inaccurate Personal Data are erased or rectified without delay.
- **Security and integrity:** DNDi implements appropriate technical security measures to ensure prevention of unauthorized or unlawful processing and against accidental loss, destruction or damage to the Personal Data, as well as unauthorized access to the equipment used for data processing. All DNDi staff members are responsible for protecting Personal Data that DNDi processes by following procedures put in place to maintain the security of all Personal Data from the point of collection to the point of destruction, as stated in the Information System and Technologies Policy.

Rights of Personal Data Subjects

Data Protection law provides Data Subjects with rights (such as right to information, access, portability, withdrawal, consent and/or objection, rectification, erasure etc.) that allow them to exert control over their Personal Data. Where DNDi is Data Controller, DNDi must enable the Data Subject to exercise these rights.

Data Subject rights are described in relevant Data Protection laws, for example:

- FADP Chapter 4 (Art. 24-29) available at: https://www.fedlex.admin.ch/eli/cc/2022/491/en
- GDPR Chapter 3 (Art. 12-23) available at: Chapter 3 (Art. 12-23) Archives - GDPR.eu

Data Subjects' rights are not absolute, but subject to limitations set forth in Data Protection laws or other applicable laws. Under certain circumstances, derogations may apply and/or DNDi may reject the Data Subject's request.

To ensure Data Subjects can enforce their rights in compliance with this policy, but also in compliance with applicable legislation, DNDi has a process in place to manage Data Subject rights which is available on DNDi Policies and Procedure SharePoint.

Appointment of DPO

To facilitate the implementation of data protection at DNDi, DNDi has appointed a DPO who is responsible for supporting DNDi Staff with the implementation of this policy and interpretation of relevant Data Protection laws. DPO is responsible for:

- Drafting and revising DNDi's Data Protection policy
- Training and advising DNDi's staff on their obligations with respect to data protection
- Supporting DNDi's staff in handling Data Subjects' requests with respect to their rights
- Monitoring compliance with Data Protection laws and policies/procedures
- In case of high risk for Data Subject, providing advice on Data Protection Impact Assessments (DPIAs)
- Reporting to Global Executive Team on risks and issues

- Serving as the point of contact between DNDi and Data Protection supervisory authorities

DPO at DNDi can be contacted at dataprivacy@dndi.org.

Appointment of DPR

To ensure compliance with EU/UK GDPR, DNDi has appointed a DPR who acts as a legal representative for DNDi in case of legal proceedings which relate to these two Data Protection legislations. The name and contacts of the DPR can be found in DNDi Data Protection SharePoint.

Maintaining records of all Personal Data processing activities

DNDi maintains records of its Personal Data processing activities. These records include the identity of the Data Controller and/or Data Processor (where applicable), descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients, storage locations, transfers, retention period and a description of the security measures in place. The register is managed by the DNDi's DPO and can be accessed via DNDi's SharePoint. The records are also shared with DNDi's DPR.

Ensuring Data Protection by design and by default

While designing systems and drafting procedures related to Personal Data processing, DNDi ensures alignment to data protection principles and that it enables Data Subjects to exercise their rights. DPO can support DNDi's staff during this process.

Data Protection Impact Assessments (DPIAs)

When, based on preliminary assessment, DNDi as Data Controller engages in any high-risk Personal Data processing, DPIAs will be conducted to understand how processing may affect Data Subjects and consult the supervisory authorities if appropriate. DPIA should be conducted notably when using new technologies, in case of large-scale processing of Sensitive Data or of large-scale and systematic monitoring of a publicly accessible area.

DNDi's obligation when delegating data processing activities to third parties

In general, DNDi is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements (which may include standard contractual clauses issued by relevant Supervisory Authorities) have been put in place. This is to ensure that Data Subjects will not be at risk of losing the protection under this Policy and applicable law.

DNDi often works with third parties to process Personal Data on its behalf, who may also work with sub-processors. In such situation, DNDi must ensure that the third party (including any sub-processors) has implemented the appropriate organizational and technical measures to adhere to the principles outlined in this policy. This is achieved by requesting the third party to complete DNDi's Data Protection and IT Security Due Diligence questionnaire. DNDi must also ensure that appropriate contractual provisions are put in place to clarify the obligations of both parties in respect to ensuring data protection.

Specific measures applicable to DNDi as Data Processor

When DNDi acts as Data Processor on behalf of another Data Controller, DNDi shall:

- process Personal Data only on instructions from the Data Controller according to the specific agreement to be set up by the Data Controller with DNDi as Data Processor;
- assist the Data Controller in fulfilling its obligations in relation to Data Subject's rights
- assist Data Controller(s) in the performance of DPIA upon Data Controller's request;
- not sub-contract processing activities to another Data Processor (i.e. sub-processor) without prior written authorization from the Data Controller. DNDi shall enter into a written contract with the sub-processor and ensure that the sub-processor is subject to the same contractual data protection obligations as DNDi towards the Data Controller.

Managing Personal Data Breach

Any Personal Data Breach must always be reported to DNDi's DPO at dataprivacy@dndi.org as soon as possible. The process to manage Data Protection Breaches is described separately in the relevant procedure available on DNDi's Policies and Procedures SharePoint. All investigations related to Personal Data Breaches will be tracked and filed by the DPO in the internal DNDi's data breach log, alongside the remediation actions taken.

Roles and responsibilities

Activity	Accountable	Responsible	Consulted	Informed
Process personal data in compliance DNDi Data Protection policy and any relevant local laws	DNDi Executive Director	All DNDi Staff	Data Protection Officer	DNDi Strategy and Performance Leader
Ensure department-specific data protection corrective actions are implemented	DNDi Global Executive Team members	DNDi Data Protection Network members	Data Protection Officer	DNDi Strategy and Performance Leader
Report Data Protection Breaches to DPO as soon as possible	Any DNDi Staff member who becomes aware of the breach		Relevant DNDi Data Protection Network members	Data Protection Officer/ DNDi Strategy and Performance Leader
Manage appointment and prioritization of work of the Data Protection Officer	DNDi Strategy and Performance Leader		Relevant DNDi Data Protection Network members	

The roles and responsibilities in managing Personal Data Breach and Data Subject requests are described in the respective SOPs.

[1] *Responsible (those who do the task), Accountable (for the decision, task being done and final approval), Consulted (provides input), Informed (needs to be updated)*

References

GDPR: https://gdpr.eu/what-is-gdpr/

FADP: https://www.fedlex.admin.ch/eli/cc/2022/491/en

DNDi Procedure for Managing Data Breaches: available on DNDi Policy and Procedures SharePoint

DNDi Procedure for Managing Data Subject Rights: available on DNDi Policy and Procedures SharePoint

DNDi Data Protection Network members: available on DNDi Data Protection SharePoint