Data Protection Policy

DND*i*'s Policies

DNDi
Drugs for Neglected Diseases *initiative*

May 2020

Table of Contents

I. Introduction

This Data Protection Policy sets out DND*i*'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 will be captured in the relevant procedures and work instructions.

Any individual at DND*i*, its regional 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 DND*i* treatments, partners, suppliers and others (as applicable).

II. Glossary

- **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 or legal person directly or indirectly identifiable via Personal Data
- **Data Subject Consent:** an affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the processing of Personal Data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. Silence or pre-ticked consent are not sufficient.
- **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
- **Personal Data:** any information relating to Data Subject, whether it relates to his or her 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 pseudonymized data which can be attributed to a Data Subject by the use of additional information (e.g. a code list); 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 DND*i* 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 or not by automated means, 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

- **Pseudoanonymization of data:** it is a security measure that may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. The reference number can be tied back to the individual however it is held separately. Pseudonymized Personal Data remains Personal Data
- **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
- **Data Protection Officer (DPO):** see Section IX for full definition

III. Legal basis for this policy

GDPR has been taken as a legal basis for this policy however DND*i* recognizes that, being established in different parts of the world (notably in Switzerland) and performing activities globally, any applicable national Data Protection laws ought to be considered in case they set forth more stringent requirements. This policy does not override any other applicable national Data Protection laws. It is also acknowledged that laws other than Data Protection (e.g. laws on clinical trials) apply in addition to this policy.

IV. Applicability

This policy is applicable globally, to all DND*i* staff and all Personal Data for which DND*i* is the Data Controller or Data Processor. Unless otherwise specified, the principles stated in this policy apply to both roles.

Applicable globally: this policy applies globally however, additional country-specific data protection requirements might apply and will be reflected in the local version of this policy and relevant procedures.

Applicable to all Personal Data: this policy applies to all Personal Data for which DND*i* is the Data Controller or Data Processor, regardless of the media on which that data is stored or whether it related to Data Subjects.

Applicable to all DND*i* staff: this policy applies to all DND*i*'s staff globally (DND*i*, its regional offices and affiliated entities) which include employees, support staff, volunteers, interns, apprentices and trainees, staff hosted by DND*i* for other organizations, agency staff employed by DND*i*, core consultants, staff seconded to DND*i* from other organizations and DND*i*'s Board, Audit Committee and Scientific Advisory Committee members.

V. DND*i*'s obligation when outsourcing data processing activities

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

DND*i* often works with third parties to process data on its behalf, who may also work with sub-processors. In such situation, DND*i* 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. DND*i* must also ensure that appropriate contractual provisions are put in place to clarify the obligations of both parties in respect to ensuring Data Protection. Regulation in terms of data protection of the country of the receiving party will also have to be adhered to.

Additionally, when DND*i* acts as Data Processor, DND*i* shall not sub-contract processing activities to another Data Processor (i.e. sub-processor) without prior written authorization from the Data Controller. DND*i* 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 DND*i* towards the Data Controller.

VI. Responsibility and accountability

At DNDi, every staff member is responsible for and must be able to demonstrate compliance with this policy:

- Executive Director: ultimately accountable for DND*i*'s compliance with data protection law
- Members of the Executive Team: accountable for data protection of data in scope of their function
- DNDi's management team (H1 and above): accountable for ensuring that procedures within respective areas of responsibility are in line with this policy and that the staff processing Personal Data are aware of them
- Data Protection Officer (DPO): responsible for overseeing DND*i* Data Protection strategy and implementation (see Section IX for further details)
- DND*i* staff processing Personal Data: responsible for ensuring data processing in compliance with this policy and other relevant procedures.

VII. Principles of Personal Data processing

Processing of Personal Data at DND*i* is oriented around the following principles:

1. Lawfulness, fairness, and transparency

DND*i* will only process Personal Data in a lawful, fair, and transparent manner in relation to the Data Subject. DND*i* will process Personal Data only if one or more of the following legitimate bases for doing so applies:

- Data Subject Consent (see definition)
- Legitimate interests of DND*i* or a third party - except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject
- Compliance with a legal obligation
- Contractual basis
- Protection of the vital interest of the Data Subject or another natural person
- Public interest

To ensure fair and transparent processing, DND*i* shall inform the Data Subject of the existence of the processing operations (see below Right to information). DND*i* shall provide any information and communication relating to processing to the Data Subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

2. Purpose limitation

DND*i* will collect Personal Data only for specified, explicit and legitimate purposes. The purposes shall be determined at the time of the collection of the Personal Data.

In limited circumstances, where DND*i* or third parties intend to process data for a purpose other than that for which the Personal Data have been collected, different factors should be considered: compatibility with the original processing, context of the data collection, nature of the data, possible consequences of the processing, possible safeguards.

3. Data minimalization

DND*i* will only collect and process Personal Data that are adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

4. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. DND*i* will take every reasonable step to ensure that inaccurate Personal Data are erased or rectified without delay.

5. Storage limitation

DND*i* only 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.

Retention period for storage of Personal Data is set for a period assessed as being adequate for processing purposes. At the end of the 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 renewed, or the data are deleted or rendered permanently anonymous. In situation when the retention period needs to be renewed, new communication will be sent to Data Subject with indication of the legal basis for such renewal.

6. Security and integrity

DND*i* has implemented and shall continue to implement 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 DND*i* staff members are responsible for protecting Personal Data that DND*i* 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 IT Policy.

VIII. Rights of Personal Data Subjects

Data Protection law provides Data Subjects with rights that allow them to exert control over their Personal Data. Where DND*i* is Data Controller, DND*i* must enable the Data Subject to exercise these rights. Where DND*i* is Data Processor, DND*i* shall assist the Data Controller in fulfilling its obligations in relation to Data Subject's rights.

Data Subjects' rights are not absolute, but subject to limitations set forth in Data Protection law or other applicable laws.

Under certain circumstances, DND*i* may reject the Data Subject's request when the exercise of their rights proves impossible, involves disproportionate efforts, adversely affects intellectual property rights, trade secret or third parties, impedes the right of freedom of expression and information, hinder the establishment, exercise or defense of legal claims, is overridden by compelling interest or undermines the achievement of the purposes for which the Personal Data are processed. Derogations to the Data Subject's rights apply mostly (but not only) when Personal Data are processed for scientific or historical research purposes or statistical purposes. Consequently, DND*i* staff should first consider all the circumstances surrounding any request made by the Data Subject.

Data Subjects can enforce their rights at any time by contacting DND*i* at dataprivacy@dndi.org. Requests from Data Subjects need to be processed within one month from the reception date. If

contacted directly, DND*i* staff members can process the request if they perceive that it is in the merit of their activities or forward to the other DND*i* staff member who owns the relationship with the Data Subject for action. In case of doubt, they can contact DPO for support in handling the request by contacting dataprivacy@dndi.org.

The identity of the Data Subject requesting Personal Data under any of the rights listed below must be checked.

1. Right to information

Right to receive the following information about data processing when their Personal Data has been obtained or collected:

- Whether DND*i* is the Data Controller
- The contact details of the DPO
- The purpose for which data is processed and legal basis for processing
- The source of data where they have not been obtained from the Data Subject
- The categories of Personal Data concerned
- Whether the data is likely to be shared with any third party or a category of third parties, and, in particular, to any third party in a third country (i.e. international transfer)
- How long the data will be stored for
- The rights described below
- The right to lodge a complaint to a supervisory authority

The information should be given to Data Subject at the time of collection from the Data Subject, or, where the Personal Data are obtained from another source, within a reasonable period, depending on the circumstances of the case.

Where the Data Controller intends to process the Personal Data for a purpose other than that for which they were collected, the Data Controller should in principle provide the Data Subject prior to that further processing with information on that other purpose and other necessary information.

2. Right to access

Right to verify own Personal Data and to be given access to it.

When applicable, DND*i* shall provide one copy of the Personal Data free of charge. For any further copies requested by the Data Subject, DND*i* may charge a reasonable fee based on administrative costs.

Data Subjects have a right to receive the information in writing (e.g. printout, photocopy). Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form.

3. Right to rectification

Right to request correction of mistakes or inaccuracies in Personal Data.

DND*i* shall communicate any rectification of Personal Data to each third party to whom the Personal Data have been disclosed unless this proves impossible or involves disproportionate effort.

4. Right to erasure (or right to be forgotten)

Right to request Personal Data to be deleted from the DND*i*'s databases when there is no legal ground or no purpose anymore for the processing.

DND*i* shall communicate any erasure of Personal Data to each third party to whom the Personal Data have been disclosed unless this proves impossible or involves disproportionate effort.

5. Right to object

Right to object at any time to the processing of the Personal Data.

The right to object is limited to three types of processing: direct marketing, processing based on legitimate interest/public interest, processing for research/statistical purposes.

6. Right to restrict processing of Personal Data.

The right to restrict processing means the marking of stored Personal Data with the aim of limiting their processing in the future and could be implemented by, inter alia, temporarily moving the selected data to another processing system, making the selected Personal Data unavailable to users, or temporarily removing published data from a website.

The right to restrict processing is basically granted in situations of contestation or dispute and allows the suspension of processing until their resolution.

DND*i* shall communicate any restriction of processing to each third party to whom the Personal Data have been disclosed unless this proves impossible or involves disproportionate effort.

7. Right to withdraw consent

This right provides the Data Subject with the ability to withdraw a previously given consent for processing of their Personal Data for a purpose. DND*i* shall stop the processing of the Personal Data that was based on the consent provided earlier.

8. Right to object to automated processing

This right provides the Data Subject with the ability to object to a decision based on automated processing. As DND*i* does not make any decisions based on automated processing at this point of time, the right is not applicable to DND*i*'s Data Subjects.

9. Right for data portability

This right provides the Data Subject with the ability to ask for transfer of his or her Personal Data. As part of such request, the Data Subject may ask for his or her Personal Data to be provided back (to him or her) or transferred to another Data Controller. When doing so, the Personal Data must be provided or transferred in a machine-readable electronic format.

10. Right to be notified of a Personal Data Breach and to complain to the supervisory authority

In case of a Personal Data Breach, DND*i* will notify the affected Data Subject as soon as possible, as outlined in Section X of this document.

If Data Subjects feel that that DND*i* does not process their data in compliance with the data protection laws, they have the right to refer the matter to the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland or to any other competent supervisory authority.

IX. Measures to reinforce Data Protection at DND*i*

To ensure adherence to the data protection principles, as outlined in Section VII, and to enable Data Subjects to exercise their rights, as outlined in Section VIII, the following measures are taken by DND*i*.

1. Appointment of DPO

To facilitate implementation of data protection at DND*i*, DND*i* has appointed a DPO who is responsible for overseeing DND*i*'s data protection strategy and implementation. In addition to supporting DND*i*'s staff in implementing measures described in this section of the policy, DPO is responsible for:

- Drafting and revising DND*i*'s Data Protection policy
- Training and advising DND*i*'s staff on their obligations with respect to Data Protection
- Supporting DND*i*'s staff in handling Data Subjects' requests with respect to their rights
- Monitoring compliance with data protection laws and policies
- Providing advice on Data Protection Impact Assessments (DPIAs)
- Reporting to Executive Team on risks and issues
- Serving as the point of contact between DND*i* and Data Protection Supervisory Authorities

DPO at DND*i* can be contacted at dataprivacy@dndi.org.

2. Maintaining register of all Personal Data processing activities

DND*i* maintains records of its Personal Data processing activities. These records include 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 DND*i*'s DPO.

3. Ensuring Data Protection by design

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

4. Implementing appropriate safeguards when sending data to Third Parties

See above, Section VIII.

5. Implementing appropriate safeguards when processing Sensitive Personal Data

The right to process of Sensitive Personal Data is more limited and subject to conditions, such as implementation of appropriate safeguards or specific legal basis. This includes processing Sensitive Personal Data for scientific, historical, research or statistical purposes where appropriate safeguards (anonymization where possible; alternatively, encryption or pseudonymization) need to be put in place.

6. Conducting Data Protection Impact Assessments (DPIAs)

When DND*i* engages as Data Controller in any high-risk Personal Data processing, DPIAs will be conducted to understand how processing may affect Data Subjects and consult the 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. A DPIA will include: 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. DPO can provide advice on conducting DPIAs.

7. Reinforcing compliance via regular trainings and internal controls

DND*i* shall ensure that all DND*i* staff has access to adequate training to enable them to comply with this policy. All DND*i* staff must undergo all mandatory data protection trainings. Furthermore, internal controls will be conducted to ensure compliance and address potential issues proactively. Both activities will be coordinated by the DPO.

8. Specific measures applicable to DND*i* as Data Processor

When DND*i* acts as Data Processor, DND*i* shall process Personal Data only on instructions from the Data Controller and inform the Data Controller if DND*i* believes that the instructions breach Data Protection law. DND*i* shall not engage with any sub-processor without prior written authorization from the Data Controller (see Section V). DND*i* shall notify the Data Controller without undue delay upon learning of Personal Data Breach, assist the Data Controller in answering the Data Subject's requests and in compliance audit.

X. Breach of Data Protection Law

Any breach of security leading to the accidental or unlawful destruction, loss or alteration of, or unauthorized access to Personal Data transmitted, stored or otherwise processed by DND*i* or by third parties on behalf of DND*i* must always be reported to DND*i*'s DPO at dataprivacy@dndi.org as soon as possible. The affected Data Subject and the relevant supervisory authority must be notified as soon as possible of a Personal Data Breach, at the latest 72 hours after learning of the breach. In addition, when DND*i* acts as a Data Processor, DND*i* shall also notify the Data Controller immediately. All investigations related to Personal Data Breaches will be tracked and filed by the DPO in the internal DND*i*'s case management system EQS.