GDPR Guideline

(hereinafter the "**Guideline**")

Purpose

The purpose of this Guideline is to define and set forth a process ensuring minimal security requirements (hereinafter the "**MSR**") of the personal data processing, to be met by INDRC, so as compliance with the requirements of the article 24 of the GDPR to be observed and to be able to be demonstrated.

Breach of this Guideline shall represent misbehavior and shall be subject to corrective and/or disciplinary procedures.

Scope

This Guideline is global in scope and applies to INDRC worldwide, all INDRC employees, subcontractors, statutory body members and member of other bodies, and external service providers of INDRC as well as other persons cooperating with INDRC, including persons cooperating with INDRC on voluntary basis. This Guideline applies also to the aforementioned individuals who are involved with the project Center for Artificial Intelligence and Quantum Computing in System Brain Research (CLARA) (hereinafter as "**Responsible persons**").

In case a Responsible person is a data processor within the meaning of article 4, paragraph 8 GDPR, a data protection agreement shall be entered into. For the avoidance of doubt, the principles of this Guideline apply to data processors as well.

Definitions

For the purposes of this Guideline:

Personal data means any information relating to an identified or identifiable natural person (hereinafter as "**data subject**"), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing / Handling means 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.

INDRC means International Neurodegenerative Disorders Research Center, zapsaný ústav.

INDRC Director means a person who was appointed an executive director of INDRC.

CLARA Director means a person who was appointed a director or interim director of the CLARA by INDRC.

The Director means INDRC Director or CLARA Director.

Principles for Processing Personal data

INDRC commits to Processing Personal data in accordance with the following principles:

a) **Lawfulness, Fairness, and Transparency**
   Personal data shall be processed lawfully, fairly, and transparently.
b) **Purpose Limitation**
   Data shall only be collected for specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
c) **Data Minimization**
   Only the data necessary for the intended purposes will be collected and processed.
d) **Accuracy**
   Personal data must be accurate and kept up to date.
e) **Storage Limitation**
   Data will not be retained longer than necessary for the purposes it was collected.
f) **Integrity and Confidentiality**
   Data will be protected against unauthorized access, alteration, or destruction.

Supervision

INDRC Director is authorized and instructed to control compliance with the provisions of this Guideline including MSR measures, unless such responsibilities are related to CLARA Project and therefore assigned to CLARA Director.

CLARA Director is authorized and instructed to control compliance with the provisions of this Guideline including MSR measures in relation to CLARA organizational unit.

The Director especially

a) strictly observes secrecy and confidentiality obligations in relation with performance of his/her role and responsibility.
b) fulfils specific responsibilities in relation with this Guideline, respectively:
   - ✓ provides the IT service providers with any necessary instructions and assistance
   - ✓ defines necessary measures to be taken
   - ✓ provides corrective and/or disciplinary procedures
   - ✓ maintains a record of all data subject requests and responses
   - ✓ responds to data subject requests
   - ✓ communicates with the Office for Personal Data Protection in all matters, including data breach notification
   - ✓ determines the dates and methods of trainings
   - ✓ promotes awareness and understanding of the risks, rules, safeguards and rights in relation to Processing
c) is obliged to observe GDPR and other applicable laws.
d) fulfils other responsibilities pursuant to this Guideline.

The Director may assign part of his/her responsibilities to a designated employee.

Responsible persons

a) strictly observe secrecy and confidentiality obligations in relation with performance of their role and responsibility.
b) are bound by confidentiality obligation during the performance of their responsibilities related to Personal data protection.

c) are obliged to observe GDPR and other applicable laws.
d) fulfil other responsibilities pursuant to this Guideline.

MSR measures

a) Identification and authentication:

- ✓ Each Responsible person shall regularly change their password to any e-mail address they use to communicate with INDRC and share Personal data.
- ✓ Proper password complexity shall be enforced.
- ✓ For data transfer shall be used secure, encrypted protocols only.
- ✓ Data at rest shall be encrypted if stored in external databases.
- ✓ Each Responsible person shall regularly update their antivirus software to ensure it has the latest virus definitions and security patches.
- ✓ The software, firmware and hardware used in the ICT systems shall be reviewed at least every six months, in order to detect vulnerabilities and flaws in the ICT systems and resolve such vulnerabilities and flaws.
- ✓ Mechanisms shall be set up that permit unequivocal, personalized identification of any user who attempts to access the ICT systems and a check to establish whether each user is authorized to do so.
- ✓ Limits shall be placed on the scope for repeating attempts to gain unauthorized access to the ICT systems. After, at most, 6 failed attempts to authenticate, the associated user ID must be blocked.

b) Organizational measures

- ✓ Data will only be shared with the Responsible Persons on a need-to-know basis.
- ✓ **Incident reporting:**
  In the case of a Personal data breach, the Responsible person shall without any delay after having become aware of it, notify the Personal data breach to the Director. The notification shall at least:
  - describe the nature of the Personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal data records concerned;
  - describe the likely consequences of the Personal data breach;
  - if possible, describe the measures that can be taken to address the Personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

- ✓ In the case of a Personal data breach, the Responsible person shall provide assistance to the Director and comply with his/her instructions.

- ✓ The Responsible persons are obliged to undergo trainings on data protection and compliance as indicated by the Director.

- ✓ Should any of the Responsible person receive a request from a data subject to exercise their rights, they shall forward the request to the Director and provide any assistance the Director may require complying with the request.

- ✓ **Other organizational measures**
  The Responsible persons must always act with due care so as not to breach any provisions of the GDPR or other data protection legislation. This includes:

- not leaving any documents, premises or devices containing Personal data unattended.
- not using applications that INDRC designates as prohibited ("**Prohibited apps**") on devices that are used for work performed for INDRC. The list of Prohibited apps is attached thereto as Exhibit A.

c) Technical measures

✓ **Back-up copies and recovery**

- a back-up copy and data recovery procedures must be kept by INDRC. The Responsible persons are not supposed to keep any Personal data.

✓ **Record of events or incidents**

- all findings from the events or incidents discovered by the Responsible person either during regular operation or test of the procedure for reporting, managing or responding to incidents shall be provided promptly to the Director, for his/her review.

Data handling principles

Should the Responsible person need to share any of the Personal data with third parties (e.g. in order to perform services for INDRC or within the fulfilment of their work tasks), they must follow the following principles:

- ✓ They must ensure that the third party adheres to similar standards as INDRC.
- ✓ They must only share the data on a need-to-know basis.
- ✓ The data must be shared through secure channels.
- ✓ In case the third party is a based in a third country (i.e. outside the EU or European Economic Area), the Responsible Person must any disclosure of the data discuss with the Director beforehand.

Updating this Guideline

This Guideline enters into effect as of January 15, 2025 and is issued in accordance with the GDPR. This Guideline may be updated, in which case, the changes contained in the update shall become effective once the relevant update is published on our website.

Exhibit A: List of Prohibited apps

- Temu
- Shein
- Tik Tok
- AliExpress