

# Privacy Policy

(hereinafter the “Policy”)

## 1. Identity of the controller

Your personal data controller under this Policy is International Neurodegenerative Disorders Research Center, zapsaný ústav, ID No.: 11883383, registered seat at Evropská 2758/11, Dejvice, 160 00 Praha 6, registered in the register of entities maintained by the Municipal Court in Prague, file No. U 1004 (hereinafter the “Controller” or “we”). We would like to present to you this Policy, which explains our procedures and methods we use to ensure sufficient security of your personal data. This Policy applies also to data processing in relation to the project Center for Artificial Intelligence and Quantum Computing in System Brain Research (CLARA).

## 2. Introduction

The legal regulations regarding personal data protection require, *inter alia*, that the data subjects be informed of the processing of their personal data (and, under certain circumstances, grant their consent to this effect) and of the transfer of their data to third parties and third countries. In accordance with Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the “GDPR”), the Controller hereby informs you of the conditions of processing of your personal data and your rights as the persons concerned within the meaning of the GDPR.

This Policy applies to the processing of personal data of all data subjects whose personal data are collected and used by us specially in relation to:

- use of our websites at [www.indrc.cz](http://www.indrc.cz) and [www.clara-center.eu](http://www.clara-center.eu)
- co-operation with the Controller
- interactions with our service providers
- interactions with our business partners
- interactions with the members of the INDRC bodies
- sales and marketing notices and online communications
- protection of our legitimate interests
- acquiring information about job candidates

## 3. Definitions and laws and regulations

“Personal data” means any information/data that can be used to identify you or that can be assigned to you as a natural person.

We process personal data in accordance with the legal regulations, especially in accordance with the Act No. 85/1996 Coll., on the legal profession, GDPR and Act No. 110/2019 Coll., on personal data processing. Any terms used in this Policy shall have the same meaning as specified in the GDPR.

## 4. How we collect your personal data

We obtain your personal data primarily directly from you, based on your interest in sharing your personal data with us.

We also obtain your personal data in the course of performance of our activities and from another third parties, your employer or business partner; we may also obtain your personal data from a publicly available database.

## **5. What personal data do we process?**

Personal data processed by the Controller include, without limitation, personal data and categories of personal data specified below. For the sake of completeness, we would like to point out that we do not process all the personal data specified below specifically in relation to you; the scope of processing of personal data is specified on the basis of the relevant interaction with you as a personal data subject.

- basic personal identification data (e.g. name, title)
- contact details (e.g. name, surname, mailing address, e-mail address, telephone number, date of birth)
- payment details related to the service provided (e.g., bank account number, details on payments made, invoices)
- data from your visit to our website (e.g., cookies, IP address, information on your device)
- data you provide for the purposes of recruitment process (e.g., information about education or work experience)
- data on IP rights, including copyright and author's rights
- any other data you provide for a specific purpose of processing at your own discretion.

## **6. Legal titles for processing**

Below, we would like to describe in more details the main categories of personal data processing, the scope of which relates to the purpose of processing as described in this Policy.

### **a) Performing our legal obligations**

While performing our services, we are obliged to comply with our statutory regulations. For this reason, we are obliged to process your personal data in accordance with the law to ensure compliance of our activities and proper provision of our services.

### **b) Performance of contractual obligations**

To perform our obligations based on an agreement concluded with you, we must be authorized to process your personal data. In cases, where the legal title for the processing is the performance of the agreement, your personal data are processed primarily within the scope given by the nature of the agreement and in the scope of the basic personal identification data.

### **c) Legitimate interest**

We wish to pursue our activities efficiently; to achieve this, we can process your personal data on the grounds of a legitimate interest. Such legitimate interest includes processing of your personal data for marketing purposes.

### **d) Performance of statutory obligations**

We must comply with various statutory obligations such as tax and accounting purposes. For these purposes we will process your personal data as our partner, supplier or counterparty.

### **e) Consent**

We process your personal data primarily for the reasons set out in Art. 6 (a) to (d) hereof; however, in exceptional cases and in cases established by law, your personal data may be processed on the basis of your consent, within the scope and for the period specified

in the relevant consent. However, you may revoke your consent at any time. We would like to inform you that the withdrawal of consent does not apply to processing of personal data that occurred before the withdrawal.

## **7. Personal data are collected and processed for the following purposes:**

Depending on your relationship with the Controller, the Controller uses the personal data we collect for a number of basic purposes:

- a) for operational day-to-day activities (e.g. marketing and sales, resource management, administrative tasks and project coordination, sponsorships, communications)
- b) for administrative operations (e.g. finance and accounting, human resources, prevention and investigatory activities)
- c) for internal operations (e.g. internal audit)
- d) administration and monitoring of Controller's networks and information systems, to the extent permitted by the applicable legal regulations
- e) protection of the Controller's property and intellectual property and monitoring compliance with legal regulations
- f) transparent communication with customers, authorities and the Controller's business partners

## **8. Purposes of processing in recruitment process**

Your personal data is being processed within the framework of recruitment process only for the purposes as stated above in Article 6 of the Policy. However, especially for the purpose of:

- performing a recruitment process in the scope of performing our legal obligations arising especially from the labor laws and GDPR and for the selection of the most suitable candidate
- performing future recruitment processes in the case of consent to participate in subsequent recruitments
- conducting satisfaction survey regarding the recruitment process
- preparation of an employment contract or other contract in the event of a positive recruitment result

## **9. Retention of personal data**

Our priority is to retain personal data only for the period necessary for the fulfilment of the specific processing purpose or for the period stipulated by the legal regulations. In case such period is not stipulated, we will not retain your personal data for longer than 3 years. For this purpose, we regularly assess the necessity of processing certain personal data. Once the data are no longer necessary for any purpose for which they were being processed in accordance with this Policy, such data will be erased.

## **10. Categories of Personal Data Recipients**

We may provide your personal data to the following categories of recipients:

- a) administrative bodies and authorities on the basis of the applicable legal regulations or in accordance with a binding decision of these authorities
- b) IT providers
- c) tax and accountant service providers
- d) external law firms

- e) congress and events organizers

## **11. Transfers of Personal Data to Third Countries**

In processing of your personal data, the Controller may transfer the personal data to persons with their registered office in the European Union or in third countries. For cases of transfer of personal data to third countries that are not subject to the European Commission's adequacy decision, the Controller has adopted all the necessary measures and guarantees to ensure an adequate level of protection of the personal data as required by the applicable laws of the Czech Republic, specifically by using standard contractual clauses on personal data protection.

## **12. Personal data security**

The Controller reasonable organizational, technical and other measures to protect personal data in order to ensure that personal data in both electronic and printed form are retained securely and protected against unauthorized access, alteration, accidental loss, destruction or disclosure. Our security measures are supported by a number of security standards, processes and procedures that we introduce for you in accordance with the best practices of care for users. These measures are regularly checked, tested and, if necessary, replaced by a newer version. Our security measures include, for example, storing the data in premises with limited and controlled access or in electronic databases secured using access rights with individual identifiers, prevention of access in case of several unsuccessful attempts to log in or inactivity and the possibility to renew locked access identifiers. Furthermore, the measures include, inter alia, the adoption of reasonable steps to ensure employee liability, regular backups, etc. We also require the above security measures to be utilized by our above-defined directly co-operating entities, who are, at the same time, also subject to a confidentiality obligation same as our own employees.

However, in view of the nature of the Internet network, we cannot completely guarantee that the absolute security of personal data transferred over the Internet will be maintained. We ask you to exercise caution when you provide personal data via the Internet. We cannot guarantee that an unauthorized third party will not gain access to your personal data in connection with their transfer. Therefore, when you provide your personal data via the Internet, consider the associated advantages and risks because, e.g., in a situation where you do not inform us in writing that you require specific security measures to be taken in relation to the transfer of certain data, we will use usual internet communication services for the transfer of this data – primarily e-mail communication.

## **13. Your rights**

In accordance with the GDPR and local legal regulations on personal data protection, you have the following rights:

- Right to rectification or erasure of any incorrect or incomplete personal data retained about you by the Controller.
- Right of access to your personal data retained by the Controller.
- The right to object to the processing of your personal data in certain cases and on legitimate grounds.
- If we process your personal data based on your consent, you have the right to withdraw your consent.
- Right to restriction of processing of your personal data in certain cases.
- The right not to be subject to automated decision-making aimed at assessing certain personal aspects concerning you, such as behavior-based analyses.

- The right to personal data portability to you or another controller, if technically feasible; this applies in cases where you provided us with your personal data with your consent or as part of a contract and your personal data are processed by automated means.
- The right to lodge a complaint with the competent national supervisory authority for personal data protection or exercise the right to compensation for damage. The Office for Personal Data Protection is the competent supervisory authority in the Czech Republic.

We also bear the notification obligation regarding rectification or erasure of personal data or restriction of processing when we shall inform you about such changes, unless this proves impossible or involves disproportionate effort.

If you wish to exercise any of your above rights and/or obtain the relevant information, you can contact us via the contact details specified below.

If you request the exercise of your rights, acknowledge that in order to verify whether the relevant request has been made by you, we may request that you provide identification information.

At the same time, we would like to point out that in view of the specific nature of our activities and overall specifics of the legal field, we do not have to comply with some of your requirements, especially those related to the legal claim represented by us.

#### **14. How can you contact us?**

If you have any questions concerning the scope, use, alteration or erasure of the personal data you provided to us, or if you wish to withdraw your consent to the processing of your personal data by us, please contact us by e-mail at: [info@indrc.cz]

#### **15. Updating this Policy**

This Policy enters into effect as of January 15, 2025 and is issued in accordance with the GDPR in order to comply with the information duty borne by the Controller under the GDPR. At the same time, we would like to inform you that this Policy may be updated, in which case, the changes contained in the update shall become effective once the relevant update is published on our website.