PERSONAL DATA PROTECTION POLICY

I. INTRODUCTORY PROVISIONS
I. I. OBJECTIVE OF THE ACT

Article 1
This Personal Data Protection Policy (hereinafter: Policy) is a basic act that describes the purpose and goals of collecting, processing, and managing personal data within a company. The policy ensures an adequate level of data protection in accordance with GDPR and other applicable laws regarding the protection of personal data, which are further ensured through other internal acts in this field. The Policy defines basic principles and rules of personal data protection in accordance with business and the safety requirements of the company, as well as legal regulations and best practices and internationally accepted standards. The aim of the Policy is to establish appropriate processes for protecting and managing the personal data of clients, employees, company business partners and other persons whose personal data are processed (hereinafter: data subjects).

I. II. OBLIGATIONS OF STAKEHOLDERS ACCORDING TO GDPR

Article 2
The provisions of this Policy must be abided by all employees on the subscription for "System for Early Neurological Deviation Detection – SENDD" service by TIS Grupa d.o.o. (Heinzelova 33, 10 000 Zagreb, Croatia) as the Data processor and Polyclinic Sabol for Children's Diseases, IV. Cvjetno naselje 21, 10 000 Zagreb, as the Data controller, which are involved in the process of collecting, processing, and managing personal data.

In accordance with GDPR, Data controller (hereinafter “controller”) take over certain obligations. Data Controller shall continuously implement appropriate technical and organisational measures considering the nature, scope, context and purposes of processing, as well as the risks of different levels of likelihood and seriousness for the rights and freedoms of the data subject.

These measures include the implementation of appropriate data protection policies:

- Data subjects’ personal data is stored in accordance with the legal obligations and internal security standards of the company. Data Controller continuously take significant technical and organizational measures to protect the personal, as well as all other, data of the data subjects. Where applicable, the Data Controller apply cryptographic methods of data protection and make continuous efforts to improve security measures. In addition, advanced tools are used to protect and prevent data leaks and to monitor critical systems within the company.
- The Data Controllers do not allow unauthorized collection, processing, or use of personal information. Data access restriction ensures we collect and give access only to data necessary to perform business tasks. Accordingly, roles and responsibilities within Data Controller are clearly defined. Data Controller employees are

strictly forbidden to use the personal data for any purpose that does not comply with the conditions defined in Chapter III.II Legality of processing.

- Personal information is protected from unauthorized access, use, alteration, and loss. Protection mechanisms are applied to personal data within Data Controller, regardless of the form in which they are stored - paper or electronic.
- Compliance with this Policy and other data protection policies and procedures is regularly reviewed and verified by the Data Protection Officer.

I. III. IMPACT ON BUSINESS PROCESS

Article 3

This Policy affects and applies to all processing of personal data within the SENDD project, except where anonymized data is processed, or processing is for statistical analysis when it is not possible to identify an individual.

II. TERMS AND MEANINGS

Article 4

Personal Information - All information relating to an individual whose identity is identified or identifiable ("data subject").

Data subject - is a person who can be identified directly or indirectly, especially by identifiers such as name, identification number, location information, network identifier, or by one or more factors specific to physical, physiological, genetic, mental, economic, cultural or the social identity of that individual.

Processing personal data - any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.

Data controller - means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor - means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Supervisory Authority - means an independent public authority which is established by a Member State and ensures the implementation of the Regulation.

Consent - any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Pseudonymization - means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

III. PRINCIPLES
III.I. PRINCIPLES OF PERSONAL DATA PROCESSING

Article 5
The Data Controller process personal data in accordance with the following processing principles:

1. **Lawfulness, fairness, and transparency** - with respect to the data subjects and their rights, Data Controller will process the personal data in compliance with the applicable laws respect to the rights of the data subjects. Processing transparency enables data subjects to get all needed information about the data processing and ensures, upon their request, an insight into their data and the processing with information about grounds and legality of processing, etc. The data subject will be informed of all relevant information in due time, preferably before the data collection itself.
2. **Purpose limitation** - Personal data must be collected for specific, explicit and legitimate purposes and may not further processed in a manner that is incompatible with those purposes, unless there are other processing that is required by law or necessary for quality delivery of services.
3. **Data minimization** – The Data Controller collect and process personal information in such a way that it is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy** –The Data Controller ensure that data is accurate and kept up to date, which means that every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased, or rectified without delay. The application of this principle is ensured by Data Controller through the implementation of regular control and an open process of communication with data subjects.
5. **Storage limitations** – The Data Controller ensures that the personal data are kept in a form that permits identification of the data subjects only for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods but there must be a clear purpose for this, in terms of legal obligation or legitimate interest.

6. **Integrity and confidentiality** – The Data Controller collect and processes information in such a way as to ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

In accordance with the above principles, personal data will be accessed by Data Controller and Data Processor employees depending on their authorizations and job description. A certain part of the processing is provided by other legal entities with whom the personal data will be shared only if they are necessary for the purposes of fulfilling the obligations of the joint agreements. The Data Controller will also forward the data of the data subjects to state institutions or associations if there is a legal basis for this.

III.II. LEGALITY OF PROCESSING

Article 6

The Data Controller consider the personal data as property of data subjects and acts accordingly.
As a result, the personal data of the data subjects are processed when at least one of the following conditions is met:

1. processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;
2. processing is necessary for compliance with a legal obligation to which The Data Controller are subject.
3. processing is necessary for the purposes legitimate interests pursued by Joint Controllers or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subjects which require protection of personal data, especially where the data subject is a child.
4. the data subject has given consent to the processing of his or her personal data for one or more specific purposes - consent must be demonstrable and voluntary, written in easy-to-understand language, and the data subject shall have the right to withdraw his/her consent at any time (withdrawal of consent must be as simple as giving consent).
5. processing is necessary to protect the vital interests of the data subject or another natural person;
6. processing is necessary to perform task of public interest or in the exercise of official authority vested in the controller.

The Data Controller is required to identify the legality of any processing that is within their business domain. In identifying the legality of the processing, Data Protection Officer will be consulted and, according to clear and predefined criteria, will advise the organizational unit of the legality of the processing.

IV. DATA SUBJECTS RIGHTS

Article 7

Data subjects, at any time, retain certain rights with respect to the processing of their data. The Data Controller collect and process personal data only when the processing is lawful.

Article 8

At the time of collecting information from the data subjects, The Data Controller will provide the following information:

- identity and contact details of the Data Controller,
- identity and contact details of the Data Processor,
- contact details of the data protection officer,
- purposes and the legal basis for the processing of personal data,
- legitimate interests,
- recipients, or categories of recipients, of personal data,
- if any, the intention to transfer personal data to third countries,
- data retention period, or criteria defining that period,
- right to withdraw the consent at any time,
- if applicable, potential automated decision making,
- rights of data subjects prescribed by GDPR,
- a source of personal information if the data are not directly collected of the data subjects.

Article 9

The Data Controller process personal data in accordance with data subject rights defined in GDPR, which relates to:

1. Right to erasure ("right to be forgotten") - the data subject has the right to obtain the erasure of personal data concerning him or her without undue delay and The Data Controller will erase personal data without undue delay if one of the following grounds is fulfilled:

a) personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
b) the data subject withdraws consent on which processing is based and there is no other legal ground for the processing,
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing,
d) personal data have been unlawfully processed,

e) personal data must be erased for compliance with a legal obligation.

2. Right of access - the data subject has the right to receive confirmation from the Data Controller whether his or her personal data are being processed, and where that is the case, access to personal data and the information about purposes of processing, categories of data concerned, potential categories of recipients to whom the personal data will be disclosed and similar.

3. Right to rectification - the data subject has the right, without undue delay, to obtain rectification of inaccurate personal data concerning him from the Data Controller. Considering the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement. In addition, data subjects have an obligation to notify from Joint Controllers of any changes of their personal information in a business relationship with the company.

4. Right to data portability - the data subject has the right to receive personal data concerning him or her, which he or she has provided to from the Data Controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another data controller, without hindrance from the controller to which the personal data have been provided. It should be in mind that the right of transfer relates solely to the personal data of the data subjects.

5. Right to object - the data subject has the right, at any time, to object to personal data processing, on grounds relating to his or her situation, at any time to processing of personal data concerning him or her. In such a case, the Data Controller may no longer process personal data unless it demonstrates compelling legitimate grounds for processing that override the interests, rights, and freedoms of the data subjects or for establishment, exercise, or defence of legal claims. In relation to the processing of personal data for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning him or her for such marketing. If the decision-making is based on automatic data processing, it will be carried out in accordance with the Regulation.

6. Right to restriction of processing - the data subject has the right to obtain from the Data Controller the restriction of processing if:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data,
- believes that processing is unlawful, and the data subject opposes the erasure of personal data and instead requests a restriction on their use instead, and
- the data subject has objected to the processing and pending the verification whether the legitimate grounds of the Data Controller override those of the data subject.

V. EXERCISING DATA SUBJECT RIGHTS

Article 10

The data subject may request the exercise of rights set out in Article 9 of this Policy at any time. the Data Controller will provide information on the undertaken actions related to the mentioned rights at the request of the data subjects no later than one month from the receipt of the request, and depending on the quantity and complexity if requests, it may be extended by a further month. If the Data Controller do not respond to the request of the data subjects, it shall inform the data subject without delay and no later than one month after receiving the request of the reasons for not acting. The reasons for not acting imply the existence of a lawful ground for processing.

Article 11

The data subject has the right to complain to the supervisory authority (Personal Data Protection Agency) in the event of an incident concerning his personal data or if he considers that from the Data Controller violate his rights as defined in the General Data Protection Regulation.

Article 12

Any person who has suffered material or non-material damage because of an infringement of GDPR has the right to receive compensation from the Data Controller or processors for damage suffered. Any controller involved in processing is liable for damage caused by processing that infringes GDPR. A processor shall be liable for damage caused by processing only where it has not complied with the obligations of GDPR specifically directed to processors or where it has acted outside or contrary to the lawful instructions of the controller. The data controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

VI. PROCESSING OF PERSONAL DATA

Article 13

The Data Controller do not process data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, or sexual orientation of an individual. Special protection is given to personal data of children under the age of sixteen. The processing of such special categories of personal data will be carried out only exceptionally and if:

- the data subject gave explicit consent to the processing of this personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out obligations and exercising special rights of Joint Controllers or data subjects in the field of employment and social security and social protection law in so far as it is authorized by Union or, the law of the Republic of Croatia or a collective agreement pursuant to Croatian law, providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or other individual;
- processing refers to personal information that is clearly published by the data subject;

- processing is necessary to establish, achieve or defend legal claims.

VII. THIRD PARTY DATA TRANSFER

Article 14

When transferring data subjects' data to external partners, the principle of processing restriction is strictly followed, with the transfer of the minimal amount of data required to realize the requested service. In addition, the Data Controller require their partner to have at least the same level of protection of personal data as within SENDD project.
Where appropriate, and solely based on the conditions set out in Article 6 of this Policy, the Data Controller shall transmit the data to third countries or international organizations. In such situations, additional controls and safeguards are applied to the transfer of personal data in accordance with the Regulation. These measures may include a legally binding and enforceable instrument, binding corporate rules, certification etc.

VIII. DATA PROTECTION OFFICER (DPO)

Article 15

The Data Controller has appointed a Data Protection Officer who is independent and as such acts in the interest of protecting the data subjects' rights and their data. It is his responsibility to ensure the application of the Personal Data Protection Policy within the company and other internal acts that define the rules of procedure for collecting and processing personal data of data subjects.
The Data Protection Officer shall be appropriately and timely involved in all matters concerning the protection of personal data. Participates in company processes concerning the management of changes and projects, which enables him to access information in a timely manner.

The Data Protection Officer shall at least:

- inform and advise the Data Controller and employees who carry out the processing of their obligations pursuant to GDPR and other provisions of the European Union or the Republic of Croatia on data protection;
- monitor compliance with GDPR and other provisions of the European Union or the Republic of Croatia data protection provisions and with the Data Controller policies relating to the protection of personal data, including assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- supervising the implementation of the management policy and the management of personal data files,
- providing advice were requested as regards the data protection impact assessment and monitor its performance;
- cooperate with the supervisory authority;

- acting as the point of contact for the supervisory authority on processing issues and advising on any other issues, as appropriate.

Article 16

To ensure his independence, the Data Protection Officer shall not receive any instructions regarding the performance of the tasks.

The Data Protection Officer may:

- contact data subjects who wish to exercise their rights related to the processing of personal data and other rights under the Regulation,
- receive inquiries and information related to the protection and processing of personal data,
- receive complaints and exercising other rights related to the protection of personal data.

The Data Controller has the right to charge a reasonable fee based on administrative costs and/or to refuse to act on the request if the requests are found without ground or unreasonable, especially if they are repeated frequently.
The contact details of the Data Protection Officer are available on the project website at send.eu and can be contacted via the email address privacy@sendd.eu.

IX. OBLIGATIONS OF DATA CONTROLLER TO PERFORM THE DATA PROTECTION IMPACT ASSESSMENT

Article 17

If it is likely, by its nature, scope, context, and purpose, that some processing will have a high risk to the rights and freedoms of the data subjects, the Data Controller will, before such processing, evaluate the impact of the intended processing operations on the protection of personal data. This assessment may refer to numerous similar processing operations that present similar high risks, and the Data Controller will, as appropriate, carry out an impact assessment on all active processing operations.
The Data Controller is, in cooperation with the Data Protection Officer, obliged to carry out an impact assessment according to the stated criteria and applicable internal acts.

The Data Protection Officer should ensure the implementation and support of a "data protection impact assessment" in the event of:

- automated processing that conducts an extensive assessment of personal aspects of individuals, including the creation of profiles, and based on decisions that produce legal effects that relate to the individual or similarly significantly affect the individual are made;
- extensive processing of specific categories of personal data;
- systematic monitoring of the publicly accessible area on a large scale
- in cases of processing prescribed by the supervisory authority (Personal Data Protection Agency).

Article 18

The impact assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purpose of the processing, including the legitimate interest pursued by the Data Controller;
- an assessment of the necessity and proportionality of the processing operations in relation with their purposes;
- an assessment the risks to the rights and freedoms of the data subjects;
- measures envisaged to address risk issues, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation, considering the rights and legitimate interests of data subjects and other persons concerned.

X. RECORDS OF PROCESSING ACTIVITIES

Article 19

The Data Controller keep a record of the processing activities for which it is responsible, such records shall be in electronic form and shall contain at least the following information:

1. the name and contact details of the Data Controller and the Personal Data Protection Officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. the categories of recipients to whom personal data have been or will be disclosed including recipients in third countries or international organizations;
5. transfers of personal data to a third country or an international organization, including the identification of that third country or international organization;
6. the envisaged time limits for erasure of the different categories of data, if possible;
7. a general description of the technical and organizational security measures, if possible.

Data Protection Officer is responsible for maintaining the processing register and all organizational units are responsible for providing accurate and timely information to adequately complete the processing register.

XI. DATA PROCESSOR'S OBLIGATIONS

Article 20

• Concerning Personal Data, the Data Processor is authorized to act exclusively according to the recorded instructions of the Controller.

• The Data Processor is not, without the permission of the Controller, authorized to collect, record, organize, structure, store, adapt or change, find, use, disclose by transmission, dissemination or otherwise making available, align or combine, limit, delete, copying or destruction of Personal Data.

• The Data Processor undertakes to ensure that all persons acting under the guidance of the Processor, who have access to Personal Data, act by this Policy and the recorded instructions of the Processor and that they undertake to maintain the confidentiality of Personal Data.

• The Data Processor undertakes to provide the Controller with all the necessary assistance to fulfil the Controller's obligation to respond to requests for exercising the data subject's rights and to ensure compliance with the Controller's legal obligations.

• Based on the instructions of the Controller, the Processor undertakes to immediately stop activities that may include viewing Personal Data or processing Personal Data.

• The Data Processor undertakes to provide all necessary technical and organizational measures for the protection of Personal Data and the prevention of Personal Data violations.

• Measures to protect the security of Personal Data include protection against unauthorized and illegal processing, reproduction of data in oral or written form, distribution to an unauthorized person, accidental and illegal destruction, loss or damage of data, illegal publication, and illegal access to Personal Data.

• Unless the information is a business secret or if the Executor may not disclose it for another reason, at the request of the Data Controller, the Data Processor undertakes to make available to the Data Controller all information and all documentation necessary to prove compliance with regulations on personal data protection, in a form acceptable to the Controller, and which enables the Controller or a third person authorized by the Controller to supervise the handling of Personal Data.

• The Data Processor may not hire another Processor without the prior written approval of the Controller.

• If the Data Processor hires another Data Processor to carry out special activities that may include viewing Personal Data, all the rights and obligations of the Data Processor and the Data Controller apply about the other Processor.

• The processor is responsible to the Data Controller for the performance of obligations by another processor, especially regarding the confidentiality of Personal Data, the protection of Personal Data, and the security of Personal Data.

• In the event of a violation of Personal Data, the Data Processor undertakes to notify the Data Controller without delay. If this is possible, in such notification the Data Processor is obliged to inform the Data Controller of the type of violation, the category and number of respondents about which the violation occurred, and the set and number of sets of Personal Data affected by the violation.

• In the event of a violation of Personal Data, the Data Processor undertakes to immediately take all necessary and reasonable measures to eliminate the violation of Personal Data and to mitigate the negative consequences of such a violation. The processor undertakes to inform the Data Controller of all measures taken as soon as possible.

• The processor undertakes to record every violation of Personal Data, including all circumstances related to the violation of Personal Data, the consequences of the violation, and the measures taken to eliminate the violation and mitigate the harmful consequences of the violation, to enable the Data Controller to record the fulfilment of all obligations regarding notification of the supervisory authorities and respondents on the violation of Personal Data.

• The Data Processor is responsible to the Data Controller for all damage that may occur due to a violation of this Policy by the Data Processor, its employees, or other persons hired by the Data Processor to fulfil the obligations under the Policy.

• With the termination of this Policy, the Data Processor's authorization to process Personal Data ends, and the Data Processor undertakes, based on the written instructions of the Data Controller, to delete, destroy or return the Personal Data to the Data Controller without delay.

XII. DATA BREACH

Article 21

The Data Controller takes appropriate technical and organizational measures to protect personal data. All Data Controllers' employees have an obligation to notify the responsible persons, especially the Data Protection Officer, in case of an incident related to the protection of personal data. In case of a personal data breach, the Data Controller will report the incident to the Personal Data Protection Agency within 72 hours after finding out about the violation, if possible.
In the event of a personal data breach that is likely to cause a high risk to the rights and freedoms of individuals, the Data Controller shall, without undue delay, inform the data subject of the breach of personal data.

The Data Controller will not notify the data subject of personal data breaches if at least one of the following conditions is fulfilled:

- The Data Controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular, those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
- The Data Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;
- it would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

XIII. FINAL PROVISIONS

Article 22

This Policy shall enter into force on the date of its adoption and shall apply from September 5, 2024.