THE CYPRUS INSTITUTE OF NEUROLOGY & GENETICS

DATA PROTECTION MANUAL

In compliance with the General Data Protection Regulation (GDPR) – Regulation (EE) 2016/679 and all its amendments and in compliance to the Cyprus Law (N125(1)/2018), the Cyprus Institute of Neurology and Genetics ("CING", "CSMM", or the "Institute") respects the Personal Data of any Data Subject it interacts with, such as patients, subjects of research programs, visitors, students, associates, collaborators and employees and has taken the necessary technical and organizational measures for their protection.

1. DEFINITIONS

1.1. **Anonymized Data** means the data or set of data that does not identify an individual and cannot reasonably be used to determine identity. Anonymization requires the removal of data that leads to the identification of a person such as the name, identification number, patient number / employee number and/or any other Personal Data or combination of Personal Data that may support identification directly or by association (e.g. using someone's initials). While determining whether a data or set of data is anonymized account should be taken of all the means reasonably likely to be used, such as singling out to identify the natural person directly or indirectly;

1.2. **ASM:** The Administrative Services Manager.

1.3. **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

1.4. **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.

1.5. **CING, CSMM, Institute** refer to the Cyprus Institute of Neurology and Genetics and to the Cyprus School of Molecular Medicine.

1.6. **Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others that determines the purposes and means of the processing of Personal Data;

1.7. **Data Flow Mapping** means the table recording the flow of an organization's data per procedure. The Data Flow Mapping documents the entry point of data, the type of processing the data undergoes and the exit point indicated in the retention period. The Data Flow Mapping is published at the CING fileserver.

1.8. **Data Protection Impact Assessment** ("DPIA") is the process defined by Article 35 of GDPR through which an Organization assesses the potential impact of a process of Personal Data taking into account the nature, scope, context and purposes of the processing, and the likelihood to affect the rights and freedoms of natural persons.

1.9. **Data Subject** means the individual (living person) who is the subject of Personal Data.

1.10. **Database** means a structured set of data held in an electronic format by a system that is accessible in various ways;

1.11. **DPO** means the Data Protection Officer, the person identified by the Organization as being the main contact regarding the protection of Personal Data

1.12. **GDPR** means "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 (General Data Protection Regulation)"

1.13. **Genetic Data** means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result particularly, from analyses of a biological sample belonging to the natural person in question;

1.14. **Personal Data** means any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly;

1.15. **Processing** 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;

1.16. **Processor** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller. It is clarified that natural persons that are acting under the capacity of the Controller, such as employees, are considered part of the Controller and not of the Processor and their actions hold liable the Controller.

1.17. **Public Authorities** means any Authority which has a legal mandate to govern, administrate a part or aspect of public life, such as all branches of the executive power of a state, province municipality, etc.

1.18. **Special Type of Data or Sensitive Data** means that Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, health information or data concerning a natural person's sex life or sexual orientation.

1.19. **Supervising Authority or Data Protection Authority or DPA** means the office of the Data Protection Commissioner of Cyprus.

1.20. **Third Countries** means the list of the counties not listed in the Official Journal of the European Union and on its website. The website lists the territories and specified sectors within a country and international organizations for which it has decided that an adequate level of protection not or is no longer ensured.

2. SCOPE OF THE GDPR:

The GDPR provisions apply to the processing of Personal Data wholly or partly by automatic means, and to the processing other than by automatic means of Personal Data which form part of a filing system or are intended to form part of a filing system.
For the purposes of the Institute, GDPR does not apply to the processing of Personal Data:

(a) by a natural person in the course of a purely personal interest;
(b) the processing performed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. GENERAL PRINCIPLES

The following principles apply in every case and the staff shall process Personal Data having always the following underlying principles in mind:

3.1 Personal Data shall be processed fairly and lawfully.

3.2 Personal Data is collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes. Personal Data can be further processed for historical, statistical or scientific reasons. Data will be kept only for the time necessary and can be further processed only for purposes related to the national security and public safety (detection of crimes etc.) only by court order, as enforced by a Cyprus relevant law.

3.3 The Processing of Personal Data (especially Sensitive Data including medical data) is confidential and shall be conducted by, assigned, dedicated personnel. All staff involved in the collection and process of Personal Data should have access only to the relevant information needed to carry out their assigned tasks.

3.4 Personal Data kept shall be relevant, appropriate and not excessive in relation to the purpose of Processing.

3.5 Personal Data shall be accurate and shall be updated when necessary to ensure it is kept up to date.

3.6 Personal Data shall be kept in a form which permits identification of Data Subjects only for the period necessary.

3.7 Personal Data that is wrongfully held and processed (without the legally accepted ways described in this document) shall be destroyed.

3.8 Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of Personal Data, against accidental loss or destruction of and /or against damage to Personal Data.

3.9 Personal Data shall not be transferred a Third Country unless following consultation with the DPO (through the ASM), pursuant to Paragraph 4.3 of this manual.

4. USING, HOLDING AND DISCLOSING PERSONAL INFORMATION

4.1. Lawful processing of personal information

In compliance with the GDPR, Personal Data may only be processed if at least one of the following conditions is met:

a) If the Data Subject has unambiguously given their consent.

b) for compliance with a legal obligation in which the Controller is subject to.

c) for the performance of a contract to which the Data Subject is party.

d) to protect the vital interests of the Data Subject or others.

e) for the performance of a task carried out in the public interest or in the exercise of public authority vested in the Institute or a third party to whom the data are communicated;

f) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by the third party to whom the Personal Data are communicated, on condition that such interests override the rights, interests and fundamental freedoms of the Data Subjects.

In addition, based on Article 9 of the GDPR, about the Processing of Special Type of Personal Data, such as physical and mental health information, the Institute is Processing lawfully when at least one of the following conditions are met:

a) the Data Subject has given explicit consent to the processing of those Personal Data for one or more specified purposes;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Institute or of the Data Subject in the field of employment and social security and social protection law;

c) processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

d) processing relates to Personal Data which are made public by the Data Subject;

e) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

f) processing is necessary for reasons of substantial public interest, on the basis of Union or Cyprus law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

g) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Cyprus law or pursuant to contract with a health professional and subject;

h) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Cyprus law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;

i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

4.2. Disclosing of Personal Data to third parties.

Where the CING transfers Personal Data outside the Institute and/or if it conducts engagements with third parties to process data on the Institute's behalf it must be ensured, via data processing agreements ("DPAs") with the third parties, that the third parties take such measures to maintain the Institute's commitment to protecting data. Third parties may include:

- Doctors/Surgeons/Physicians
- Laboratories
- Other medical centers
- Insurance companies
- Education Services
- Other Educational Institutions
- Other service providers

The third parties do not include Public Authorities, Courts and the Police.

Such Agreements are made available by the DPO through the ASM. A list of the organizations with which the Institute has signed DPAs shall be published internally by the ASM and be updated on a regular basis. Any CING staff shall check the list before sharing information with a third party.

Regarding results of medical examinations / laboratory results from/ to the CING may be sent to certified health professionals after the subject has been informed. In general, such an information is provided in the Privacy Policy published by CING. A good practice would be to verbally inform the patient about the transfer provided that the patient is in contact with CING at any point of the procedure. The results may be sent:

(a) by email; where possible with the use of encryption.
(b) by fax; the CING sender confirms the fax number of the certified receiver by phone and may arrange specific time to send the fax.

All emails with the abovementioned results are sent with the use of a central email account. Each laboratory has its own central email account used only to send laboratory results to the patients. Laboratory staff are advised to only use the central email address when they are sending results.

4.3. Disclosing of Personal Data to third parties in Third Countries.

CING should take measures to compensate for the lack of data protection while transferring Personal Data in an organization based in a Third Country by way of appropriate safeguards for the Data Subject.

Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by the Supervisory Authority or contractual clauses authorized by the Supervisory Authority.

In case that it is required to transfer Personal Data to an Organization in a Third Country the DPO should be consulted, through the ASM who will provide the appropriate safeguard method.

The ASM will publish in the fileserver of CING a list of entities in Third Countries that have been authorized by CING for such transfers. In case there is a need for a transfer of Personal Data outside the list, the ASM shall be contacted prior to such transfer.

4.4. The duty to inform:

The Institute has the obligation to inform the Data Subjects at the collection time and at any other given point about the processing of their Personal Data. The obligation is valid independently of the lawful basis (please refer to Paragraph 4.1).

The Institute has published Privacy Notices at www.cing.ac.cy to inform the Data Subjects about the processing details and their rights. Further, the Data Subjects can contact the DPO for any question, information or request regarding the Personal Data processed by CING. The contact details of the DPO are listed in this manual as well as in the Privacy Notice.

Individuals are provided with information about their participation in research projects at the time they provide their consent to the collection and processing of their personal data, pursuant to Paragraph 4.1(a) of this Manual. The information includes details of the research program and at least the following:

- Details regarding the CING (that acts as a Controller).
- Purpose of Personal Data Processing
- With whom the Personal Data might be shared with
- Where the Personal Data will be stored
- The rights related to the Personal Data held
- For how long the Personal Data will be held
- If applicable, how will the Personal Data be destroyed
- DPO contact details to whom they could ask for more information or report complaints regarding the Personal Data
- Contact details of the Supervising Authority where the individuals can file a complaint.

4.5. Adequate, relevant and not excessive

The minimum amount of identifiable Personal Data should always be processed, and the use of that information justified. The Personal Data per process (purpose) that is considered as the necessary data to be collected is included in the Data Flow Mapping. Where possible, Personal Data should be Anonymized, as this can be used with fewer constraints. Anonymization is performed for the statistical processing at the Institute.

4.6. Accurate and up to date Personal Data for patients

Patients' details must be checked from time to time (e.g. their address), and their files must be updated accordingly. It is the CING's responsibility to maintain accurate data whereas it is the Data Subject's responsibility to inform the CING for any changes.

4.7. Confidentiality of Personal Data

Personal Data should be considered as confidential in all cases. This means that CING staff is not allowed to disclose any Personal Data to a third party unless it is a lawful transfer as per the processes defined by CING or with the explicit consent of the Data Subject. Such data might be the employee files, student records or medical records.

CING staff involved in the collection and process of Personal Data should have access only to the relevant information needed to carry out their assigned tasks. For instance, the administration staff responsible for invoicing the patients should only have access to a patient contact details, and the type of examinations made to a patient and not the results or medical reports as these are irrelevant to the invoicing process.

In cases where a patient is referred for laboratory exams at a CING laboratory by a doctor outside CING, the medical reports can be given only to the patient's referring doctor and to other doctors indicated by the patient in writing. Only in exceptional cases, for the protection of the patient's health and under the responsibility of the laboratory's Head, laboratory reports can be given directly to the patient.
Third parties may collect a patient's medical report only after the patient's written authorization.

4.8. Retention and disposal of Personal Data

Personal Data should not be retained for longer than necessary. GDPR requires to process (including archiving) Personal Data for the minimum period required as determined by CING's policies. The relevant retention periods that can also be found at the Data Flow Mapping, published internally by the ASM.

Often, CING examines genetically transmitted/inherited diseases; hence in some cases it is justified to keep patients' medical data for an indefinite period. In cases where the holding and processing of Personal Data is no longer justified, the Head of the involved department/clinic is responsible for the destruction of such data.

4.9. Using patient Personal Data for Education & Training purposes

Anonymized records will usually be sufficient for use in teaching purposes and education. If it is not possible to anonymize the records, then explicit consent is needed from the patient for the use of their Personal Data restrictively for Education and Training purposes.

Students of the Cyprus School of Molecular Medicine (CSMM) and other trainees/students that participate in research projects and/or operate within Departments/Clinics should have access only to information necessary for completing the task assigned to them by the CSMM faculty (if applicable) or by the CING responsible personnel. The Heads of Departments/Clinics should always be fully informed regarding

any access students/trainees might have to Personal Data of patients within their departments and should authorize students'/trainees' access.

Students of the CSMM and other Students/Trainees must sign a confidentiality statement provided to them by the Health, Safety & Quality Office.

4.10. Video recording and Photographing

Video recording and photography of patients, visitors, students or staff by the CING or/and a media company is prohibited unless a previous written consent is signed by the individual. For persons under 18 years of age, or patients who are unable to give consent, the parent or guardian must sign the consent.

All film crews and photographers must always be accompanied by a member of the CING staff, both within or outside the Institute premises, when video recording/photographing any person that provided a relevant consent to the CING.

4.11. Personal Data of the deceased

Although Article 27 of GDPR states that the provisions of GDPR do not apply for the Personal Data of the deceased. However, CING protects and provides similar technical measures to the Personal Data of the deceased as it does for the living subjects. As such, CING does not transmit Personal Data of the deceased to any third parties, unless there is a legal reason to do so.

5. INFORMATION MAPPING

Information flows are identified for CING Labs and Clinics. Any changes should be communicated to the DPO via the ASM by the department/ clinic Heads. This is to ensure that we:

- Keep personal information secure.
- Know for what purpose we are using personal information
- Comply with the GDPR and follow guidelines in this manual
- Allow the satisfaction of the Data Subject rights

6. RIGHTS OF DATA SUBJECTS

6.1. Data Subject Rights Overview

The rights of the Data Subjects are:

- **Right to be informed:** Data Subjects have the right to be informed about the collection and use of their Personal Data. This is a key transparency requirement under the GDPR.
- **Right to access:** Data Subjects have the right to access their Personal Data. This is commonly referred to as subject access.
- **Right to rectification:** Data Subjects have the right to have inaccurate Personal Data rectified or completed if it is incomplete.
- **Right to erasure:** Data Subjects have the right to have their Personal Data erased. The right to erasure is also known as 'the right to be forgotten'.
- **Right to restriction of processing:** Data Subjects have the right to request the restriction or suppression of their Personal Data. When processing is restricted, you are permitted to store the Personal Data, but not use it.
- **Right to restriction to data portability:** This right allows individuals to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without affecting its usability. The right only applies to information an individual has provided to CING.
- **Right to object:** Data Subjects have the right to object to the processing of their Personal Data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In other cases where the right to object applies the Institute may still be able to continue processing if it can show that it has a compelling reason for doing so.

The rights can be exercised by any Data Subject in person or by a person authorized by the Data Subject. The authorized person (Data Subject in person, authorized third party or parent/guardian) shall be identified through the presentation of a satisfied method of identification as per the next paragraph of this document "Identification of the Requestor".

Any CING staff shall refer to the Data Subject Rights' Request form in APPENDIX I of this manual when they receive a Data Subject Request. All requests must be submitted by the applicants in writing and in general CING shall respond within 30 days.

6.2. Identification of the requestor

Individuals are only entitled to exercise any of their rights to their own Personal Data, and not to Personal Data relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that CING establishes whether any request received is related to the requestor's Personal Data as defined in this manual. For example, a husband is not entitled to have access to his wife's medical examinations and vice versa.

If the CING staff receiving the request has doubts about the identity of the requestor, he/she can ask for more information. However, it is important that he/she only requests information that is necessary to confirm the identity of the requestor.

CING must let the individual know as soon as possible whether additional information is needed to confirm their identity, before responding to their request. The period for responding to the request begins when CING receives the additional information.

Unless known to the CING staff receiving the request, the Data Subject making a request for exercising any of his/her rights mentioned above for his/her own data must provide proof of their identity in the form of either their identification card, passport or driving license.

Likewise, in case the Data Subject has provided his/her request through a third party, a power of attorney or a written authorization signed by the Data Subject should be provided. In such a case the identity of the third party shall be proven by the CING staff through providing their identification card, their passport or driving license.

In cases where an individual does not have the mental capacity to manage their own affairs, a court order is necessary to enable a third party to exercise subject access rights on behalf of such an individual. The same applies to a person appointed to make decisions about such matters.

In the case that the Data Subject is a minor (under 18), the request can only be received by the holder of parental responsibility over the child, who shall be identified in a similar manner as described above for the identification of the Data Subject itself.

Data Subjects may launch a request over the phone only for exercising the right to rectification. Over the phone the requestor must provide their ID number and an additional form of identification (e.g. date of birth) that can be checked by the CING staff. All other rights' requests will only be processed if submitted in writing.

In general, all Requests shall be fulfilled without any cost to the Data Subject, unless the provisions listed in the Data Subjects Rights Exceptions apply.

6.3. Data Subject Rights Exceptions

In case CING considers that a request is manifestly unfounded or excessive it can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

For either of the cases CING will need to justify its decision, thus the DPO shall be informed accordingly and the Director of Administration and Finance shall provide approval.

Additional exceptions to exercising Data Subject rights that can lead to a refusal of their exercise may be that there are applicable Cyprus Laws to safeguard the:

a) national security

b) defense;

c) public security

d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e) other important objectives of general public interest of the Union or of Cyprus, in particular an important economic or financial interest of the Union or Cyprus, including monetary, budgetary and taxation a matters, public health and social security;

f) protection of judicial independence and judicial proceedings;

g) prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h) monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i) protection of the Data Subject or the rights and freedoms of others;

j) the enforcement of civil law claims.

6.4. Right to be informed

Any Data Subject has the right to be informed about how their data is processed. This is designed to ensure transparency over how Personal Data is used and encompasses CING's obligation to provide 'fair processing information'. CING provides information to the Data Subjects by publishing Privacy Notices on its website that is regularly updated (www.cing.ac.cy)

The Data Subjects have the right to be informed about the use of their Personal Data at the time of collection and at any given time thereafter. Therefore,

1. Updated versions of the CING Privacy Notices shall be always posted on the website;
2. Any forms, electronic or physical, that are used to collect data shall indicate links to the Privacy Notices;
3. In case the data is collected over the phone or verbally / directly by CING staff, the Data Subject shall be informed at the time of collection that he/she can access details of the way his/her Personal Data is used by visiting CING's website.

The same right applies in case the Personal Data has been collected via a third party and not directly by the Data Subject, making reference to the Privacy Notices of CING.

6.5. Right to Access

The right of access, commonly referred to as subject access, gives the Data Subjects the right to obtain a copy of their Personal Data as well as other supplementary information. It helps individuals to understand how and why the Institute is using their data, and check that it is doing it lawfully.

Individuals have the right to obtain the following:

- confirmation that the CING is processing their Personal Data;
- a copy of their Personal Data;

In addition to a copy of their Personal Data, the Institute shall also provide individuals with the following information:

- the purposes of the Processing;
- the categories of Personal Data concerned;
- the recipients or categories of recipient CING discloses the Personal Data to;
- the retention period for storing the Personal Data
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the Supervisory Authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards CING provides if it transfers Personal Data to a Third Country.

CING shall provide access to a third party without the authorization of the Data Subject in case the vital interest of the Data Subject or of another individual entails so.

6.6. Right to Rectification

Data Subjects have the right to have inaccurate Personal Data rectified. An individual may also be able to have incomplete Personal Data completed. This right has close links to the accuracy principle of the GDPR. If the Institute receives a request for rectification it should take reasonable steps to verify that the data is accurate and to rectify the data if necessary. It should take into account the arguments and evidence provided by the Data Subject.

What steps are reasonable will depend, in particular, on the nature of the Personal Data and what it will be used for. The more important it is that the Personal Data is accurate, the greater the effort the Institute should put into checking its accuracy and, if necessary, taking steps to rectify it. For example, CING shall make a greater effort to rectify inaccurate Personal Data if it is used to make significant decisions that will affect an individual or others (such as data relating to a disease mis-diagnosed), rather than trivial ones (such as the mailing address of an employee or a student).

In case the Personal Data to be corrected is an opinion (such as a doctor's opinion), the opinion shall not be removed from the patient's file but an "updated" opinion shall be added, as long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is (e.g. Doctor), it may be difficult to say that it is inaccurate and needs to be rectified.

If CING has disclosed the Personal Data to others, it must contact each recipient and inform them of the rectification or completion of the Personal Data - unless this proves impossible or involves disproportionate effort. If asked to, CING must also inform the individual about these recipients.

6.7. Right to Erasure

Individuals have the right to have Personal Data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Data Subjects have the right to have their Personal Data erased if:

- the Personal Data is no longer necessary for the purpose which the Institute originally collected or processed it for;
- the specific process relies on consent as the lawful basis for holding the data, and the individual withdraws their consent (e.g. sms or email notifications);
- the Institute relies on legitimate interests as the basis for Processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

- CING processes the Personal Data for direct marketing purposes and the individual objects to that Processing;

- CING has processed the Personal Data unlawfully.

- Erasure is a legal obligation.

- The process of Personal Data concerns or results to the offer of information society services to a child (under 18 years old).

There are circumstances where CING shall notify other organizations about the erasure of Personal Data:

- the Personal Data has been disclosed to others; or

- the Personal Data has been made public in an online environment (for example on social networks, forums or websites).

In cases that the Institute has disclosed the Personal Data to others, it must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the Institute must also inform the individuals about these recipients.

Where Personal Data has been made public in an online environment reasonable steps should be taken to inform other Controllers who are processing the Personal Data to erase links to, copies or replication of that data.

The Institute must also take steps to ensure erasure from backup systems as well as production systems. The Institute must be clear with Data Subjects as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems. It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten. To manage erasure from backups, the Institute shall put the backup data 'beyond use', even if it cannot be immediately overwritten. Therefore, it shall ensure that it does not use the data within the backup for any other purpose, i.e. that the backup is simply held on your systems until it is replaced in line with an established schedule.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;

- to comply with a legal obligation; (e.g. the tax details of an employee cannot be deleted before the retention period even if there is a request to erase).

- for the performance of a task carried out in the public interest or in the exercise of official authority; (e.g. following the guidelines of Ministry of Health).

- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

- for the establishment, exercise or defense of legal claims.

In terms of Sensitive Data, the following are exempted for applying the Right to Erasure:

- if the processing is necessary for public health purposes in the public interest (eg protecting against serious threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine (e.g where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g a health)

Due to the complexity in assessing whether a request to erasure is legitimate or whether it falls within the exemptions, such requests shall be escalated to DPO through the ASM to handle.

6.8. Right to Restrict Processing

The Data Subjects have the right to restrict the processing of their Personal Data in certain circumstances. This means that an individual can limit the way that the Institute uses their data. A request might be indefinite or for a certain period of time.

The Data Subjects can request to restrict the Processing of their Personal Data in the following circumstances:

- the individual contests the accuracy of their Personal Data
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- the Institute no longer needs the Personal Data, but the Data Subject needs to keep it in order to establish, exercise or defend a legal claim; or

While the request to restrict processing is examined, CING should automatically restrict the processing whilst considering its accuracy or the legitimate grounds for processing the Personal Data in question. Once the Institute has decided on the accuracy of the

data, or whether there are legitimate grounds overriding those of the individual, it may decide to lift the restriction. In such a case, the Institute must inform the individual before it lifts the restriction.

Restriction means:

- temporarily moving the data to another processing system to avoid the main Processing;
- making the data unavailable to users; or
- temporarily removing published data from a website.

Please note that a Request to Restrict Processing is not equivalent to a Request to Erasure. In other words, Personal Data shall not be deleted in response to a Request to Restrict Processing.

Following a legitimate Request to Restrict Processing, the Institute must not process data in any way except to store it unless:

- the Institute obtains the individual's consent about the particular processing after the request to restrict;
- it is for the establishment, exercise or defense of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Following a Request to Restrict Processing, CING must contact each recipient (other entity) of such Personal Data and inform them of the restriction of the Personal Data - unless this proves impossible or involves disproportionate effort.

Due to the complexity in assessing whether a request to restrict is legitimate or whether it falls within the exemptions, such requests shall be escalated to the DPO through the ASM to handle.

6.9. Right to Data Portability

The right to data portability gives the Data Subjects the right to receive Personal Data they have provided the Institute in a structured, commonly used and machine-readable format. It also gives subjects the right to request CING to transmit this data directly to another Controller. Such a transition shall be performed provided if it is technically feasible, but the Institute shall not put in place any legal, technical or financial obstacles which would slow down or prevent the transmission of the Personal Data to the individual, or to another organization.

The right to data portability applies only when:

- the lawful basis for processing this information is the consent or for the performance of a contract; and
- the processing is carried out by automated means (i.e. excluding paper files).

However, there may be legitimate reasons for which the Institute cannot undertake the transmission. For example, if the transmission would adversely affect the rights and freedoms of others. It is however the Institute's responsibility to justify why these reasons are legitimate and why they are not a 'hindrance' to the transmission.

The right does not apply to anonymized data that, for example, CING uses for statistical or research purposes.

Due to the complexity in assessing whether a request to portability is legitimate, or whether it falls within the exemptions, such requests shall be escalated to the ASM and to the DPO to handle.

6.10. Right to Object

Data Subjects have the right to object to the Processing of their Personal Data. This effectively allows individuals to ask the Institute to stop Processing their Personal Data.

Individuals have the absolute right to object to the Processing of their Personal Data if it is for direct marketing purposes including any profiling of data that is related to direct marketing. Absolute means that the Institute cannot refuse at any ground and with any argument the exercise of this right and there are no exemptions; thus, it shall stop any direct marketing activities.

The Institute may not allow the exercise of the right to object if the Processing is performed for:

- a task carried out in the public interest;
- the exercise of official authority vested in the Institute; or
- the legitimate interests of the Institute (or those of a third party)

Also, the Institute can continue processing if:

- it can demonstrate compelling legitimate grounds for the Processing, which override the interests, rights and freedoms of the individual; or
- the Processing is for the establishment, exercise or defense of legal claims.

In such a case the Institute shall inform the individual about its decision to continue the processing, the grounds of the decision, their right to make a complaint to the Supervisory Authority and their ability to seek to enforce their rights through a judicial remedy.

In the cases that the purpose of the Processing is scientific or historical research, or statistical purposes, the right to object is more limited. An individual must give specific reasons as to why they are objecting to the processing of their data. These reasons should be based on a case to case basis.

Due to the complexity in assessing whether a request to portability is legitimate or whether it falls within the exemptions, such requests shall be escalated to DPO through the ASM handle.

6.11. Statutory timescales for complying with requests

CING must act on any request without undue delay and at the latest within one month of receipt of such request. One shall calculate the time limit from the day after they receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, one has until the next working day to respond.

6.12. Keeping an audit trail of requests from third parties

All subject access requests and requests from third parties will be kept by the ASM in a special Subject Rights Request Registry so that the Institute has an audit trail of actions taken in response to a request.

The record must include:

a. Type of request
b. Date recorded
c. Method received (in writing, verbally, via phone)
d. Details of the request
e. Contact details of the Data Subject
f. Contact details of the Requestor
g. Evidence sought and obtained to verify their identity
h. The decision to satisfy the Request or not
i. The reasons for the decision and
j. The date of fulfilling the request of informing of the decision

The Registry shall be regularly updated by the ASM. It is confidential and nobody but the ASM and the DPO shall have access to it.

7. DATA SECURITY

All CING employees, and CSMM students must follow the Information Security Policy set by the IT Office of CING. All employees are instructed to store files or written information of a confidential nature, including Personal Data, in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc. when unattended. No files or written information of a confidential nature are to be left where they can be accessed by unauthorized people.

Where data is computerized, it should be password protected or encrypted both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, those media must be kept in a locked filing cabinet, drawer, or safe.

Employees must always use the passwords provided by the IT office to access the computer system and not abuse them by passing them on to people who should not have them.

Personal Data should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorization has been received. Where Personal Data is recorded on any such device it should be protected by:

- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system — a folder should be created to store the files that need extra protection, such as medical results or information on minors. All files created or moved to the folder should be automatically encrypted
- Ensuring that laptops or USB drives are not left where they can be stolen.

8. DATA BREACH NOTIFICATION PROCESS

8.1. Data Breach definition

The GDPR introduces the requirement to notify the Supervisory Authority and, in certain cases, to communicate the breach to the individuals in case of a Data Leakage or a “Breach”.

Breach can be:

- “Confidentiality breach” - where there is an unauthorized or accidental disclosure of, or access to, Personal Data.
- “Integrity breach” - where there is an unauthorized or accidental alteration of Personal Data.

- "Availability breach" - where there is an accidental or unauthorized loss of access to, or destruction of, Personal Data. A breach will be regarded as an availability breach when there has been a permanent loss of, or destruction of, Personal Data.

8.2. Data Breach actions

In case of any report of a Breach or indication of a Breach, the ASM and subsequently the DPO shall be notified immediately.

CING shall without undue delay and, not later than 72 hours after having become aware of the breach, notify the Personal Data Breach to the Supervisory Authority, through the DPO. Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Such notification may result in an intervention of the Supervisory Authority in accordance with its tasks and powers laid down in GDPR.

"Becoming aware" is considered the time at which the Institute's staff, believe with a reasonable degree of certainty, that a security incident has occurred that has led to a compromise of Personal Data. A Controller is considered to be "aware" of a particular Breach depending on the circumstances of the specific Breach. In some cases, it will be relatively clear from the outset that there has been a Breach, whereas in others, it may take some time to establish whether any Personal Data has been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether Personal Data have indeed been breached, and if so, to take remedial action and notify when and who is required.

Once there is a report or an indication for a Breach that has been escalated to the DPO, the DPO will undertake a short period of investigation to establish whether or not a breach has in fact occurred. During this period of investigation, the Institute may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a Breach has taken place; a more detailed investigation can then follow.

Whilst it is the responsibility of CING to put in place suitable measures to be able to prevent, react and address a breach, the following guidance must be followed in case of a Breach:

- Information concerning all security-related events should be directed towards the DPO through the ASM with the task of addressing incidents, establishing the existence of a Breach and assessing risk.
- The DPO with the assistance of involved with the breach employees will perform a risk assessment to assess the level of risk to the affected Data Subjects

(likelihood of no risk, risk or high risk), keeping the relevant departments of the Institute informed.

- When required, a notification for the Breach will be sent to the Supervisory Authority and the affected Data Subjects will be informed.
- At the same time, the Institute shall act to contain and recover the Breach.
- The DPO shall document all actions taken for managing the Breach and will be responsible for running any required assessments. All documentation related the Data Breaches must be provided to the ASM for filing.

In the cases where the Institute is a Controller and uses a Processor for some processing (i.e. another entity e.g. an external laboratory), it is the Processor's responsibility to inform the CING "without undue delay" of any Breach of Personal Data they become aware. The Processor does not need to first assess the likelihood of risk arising from a breach, before notifying the Controller (CING in this case); it is the Institute that must make this assessment when they become aware of the Breach. The Processor just needs to establish whether a Breach has occurred and then notify the Institute. The Controller uses the Processor to achieve its purposes; therefore, in principle, the Controller will be considered "aware" once the Processor has informed it of the Breach. The reverse applies in the cases that CING is the Processor and another entity is the Controller.

In certain cases, as well as notifying the Supervisory Authority, when acting as a Controller the Institute is also required to communicate a Breach to the affected Data Subjects. The DPO will assess whether this is required or not. If needed, the CING will consult the Supervising Authority before making a decision. In general, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, the Institute shall communicate the Personal Data Breach to the Data Subject without 'undue delay'.

8.3. Data Breaches Reporting and Documentation

The Institute shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. That documentation shall enable the Supervisory Authority to verify compliance with the GDPR in case of an audit.

- The documentation shall include i) causes, ii) description of the incident, iii) the types of Personal Data affected and iv) the effects and consequences of the breach, along with the remedial action taken by the Institute.
- The Institute must document the reasoning behind any decisions made in response to a Breach. Specifically, if it is decided that a breach should not be notified for, the justification for that decision should be documented. This should include reasons why CING considers the Breach to unlikely to result in a risk to the rights and freedoms of individuals.

- Where CING notifies a Breach to the Supervisory Authority, but the notification is delayed, it must be able to provide reasons for the delay. It is important to provide documentation relating to this as it could help demonstrate that the delay in reporting is justified and not excessive.
- Where the Institute communicates a breach to the affected individuals, it should be transparent about the Breach and communicate in an effective and timely manner and it shall also include it in the documentation.

The retention period for the documentation of the Incidents is 10 years from the date of final conclusion of an investigation, report and management of an incident by CING provided that there have been no outstanding claims, complaints or ongoing investigations by a third party such as affected Data Subjects, their legal representatives, the Authorities, the Police, or others.

9. RESPONSIBILITIES WITHIN CING

9.1. Board of Directors

As CING is noted as the "Controller" of all Personal Data held by CING, the CING Board of Directors is ultimately legally responsible for the compliance of CING with the GDPR.

9.2. Data Protection Officer (DPO)

The data protection officer has the following responsibilities:

- to inform and advise the Institute and the employees who carry out processing of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation and with the policies of CING in relation to the protection of Personal Data, suggesting assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested by the Departments as regards the Data Protection Impact Assessment and monitor its performance;
- to prepare relevant documentation, as needed, related to the protection of Personal Data.
- To update the Data Flow Mapping when needed in cooperation with the ASM and the involved departments.
- To perform audits within the CING to ensure compliance with the GDPR.

- to act as the contact point with the Supervisory Authority on issues relating to processing, including the prior consultation, if any, and to consult where appropriate, regarding any other matter.
- to inform and advise the Board of Directors, though the Internal Audit Committee, on any matters he/she deems necessary.

9.3. Internal Audit Committee

The Internal Audit Committee is responsible for raising issues to the Board of Directors as appropriate, based on information received by the DPO, the CING Internal Auditors, or any member of the CING staff.

9.4. Administrative Services Manager ("ASM")

The Administrative Service Manager has the following responsibilities regarding Personal Data:

- Make available the list of authorized Personal Data recipients (i.e. third parties that have signed a DPA)
- Archiving the Data Flow Map and Data Privacy Impact Assessment
- Referring any questions regarding the protection of Personal Data and any other relevant issues to the DPO

9.5. Heads of Departments/Clinics.

Heads of Departments/Clinics are responsible for:

- Taking all the necessary organizational measures, following direction and advice by the DPO, regarding the processing of Personal Data and to make available to the DPO any requested resources to allow the DPO fulfill his/her duties.
- Ensuring that all staff, students and trainees within their departments, comply with the legislation and CING policy, and that key staff attend training when necessary.
- Ensuring security of Personal Data stored digitally or electronically are secure and access to it is limited to the authorized personnel as per CING's policy.
- Notifying the DPO, through the ASM regarding any changes in the filing system/s under their responsibility.
- Notifying the DPO through the ASM for any changes in the processing performed.
- Get consultation from the DPO through the ASM to report plans for the introduction of a new system/process to cater for Personal Data protection ("Privacy by Design").

- Running the Data Privacy Impact Assessment (DPIA) of the processes that are eligible for DPIA and are under their departments, following the guidelines of the DPO.

9.6. All Staff

All Staff must:

- adhere to the confidentiality clause in their contracts
- attend relevant training
- report any breaches of confidentiality
- follow the procedures set in the manuals and adhering to the policies communicated to them or published by CING.
- Handling Personal Data requests by subjects as per the procedure set herein.
- Report to the ASM & DPO any incident that they come across that violates the policies set regarding the protection of Personal Data.

THE CYPRUS INSTITUTE OF NEUROLOGY & GENETICS
P.O.Box 23462, 1683 Nicosia, Cyprus
Tel.: (+357) 22 358 600 / (+357) 22 392 600
Fax: (+357) 22 358 237 / www.cing.ac.cy

Appendix 1

Data Subject Request Form

Data Subject's Information (i.e. whose data the request is about):

Name:	ID number:
Telephone number:	Date of Birth:

What best describes the Data Subject's relation to the Cyprus Institute of Neurology and Genetics?

Patient		Employee	
Student		Past employee	
Supplier		Collaborator	
Other (Please specify)			

Requestor's Information (In case that the requestor is other than the Data Subject.)

Name:
Date of Birth:
ID/Passport number:

In case that the requestor is other than the Data Subject, please indicate with a tick (√) whether you are the holder of parental responsibility or indicate the type of written form of authorization by the Data Subject you provide:

Holder of Parental Responsibility	
Signed Authorization by the Data Subject	
Power of Attorney	

Please tick (√)the type of document you present CING with as a proof of identification of the requestor:

ID	
Passport	
Driver's License	

Signature of the Requestor Date

Type of Request Form:

(Please mark with X the right to wish to exercise. If you require any additional information, please read the Institute's policy found at www.cing.ac.cy)

Right to be informed: (Information on the processing the Data Subject's personal data undergoes)	☐	**Right to access** (Copy of the Data Subject's personal data)	☐
Right to rectification: (Update/correct the Data Subject's personal data)	☐	**Request for erasure/Right to be forgotten**: (Deletion of the Data Subject's personal data)	☐
Right to restrict processing: (Restriction of processing of the Data Subject's personal data)	☐	**Right to portability**: (Transfer of the Data Subject's personal data to another organization)	☐
Objection (Objection to data processing/ withdrawal of previously given consent)	☐		

Please provide details of your request.

Signature _____ Date _____