



INL DATA PROTECTION REGULATION REG/DIR/003

Concerning the protection of natural persons with regard to the processing of personal data by the International Iberian Nanotechnology Laboratory ('Data Protection Regulation')

CONTENTS

1.	Preamble	3
2.	Purpose and Scope.....	3
3.	Definitions.....	3
4.	Principles	4
5.	Rights of the data subject	5
6.	Personal Data Processing Rules.....	7
7.	Grounds for the processing of Special Categories of Data	8
8.	CCTV	8
9.	Data Processing for research, scientific or statistical purposes	9
10.	Transfer of personal data outside INL	9
11.	Confidentiality and security measures.....	10
12.	Storage of Personal Data	11
13.	Notification of Data Breaches.....	11
14.	Data Protection Impact Assessment	11
15.	Data Protection Team	12
16.	Duties of the Data Protection Team	12
17.	Dispute Resolution	13
18.	Omissions and Revision	13
19.	Entry into force.....	13

1. Preamble

- 1.1. INL is an international organisation dedicated to explore, articulate and deploy nanoscience and nanotechnology for the benefit of society. This is carried out through (i) engagement with society at large and in partnership with the industry and converting knowledge in economic value and employment, (ii) the training of researchers involved in the nanotechnology industry and (iii) the analysis, prevention and mitigation of the nanotechnology emerging risks.
- 1.2. In the context of its activity, INL processes Personal Data, pertaining both to its Members of the Personnel, and to other natural persons with whom they relate, including partners, customers, suppliers' representatives, members of academic, technological and research institutions, as well as members of the public.
- 1.3. Due to the status of INL as an intergovernmental organisation, INL is deemed a third party under the GDPR for personal data purposes. However, INL undertakes that all issues related to the processing of personal data are regulated by the highest available standards, including the requirements set forth in the GDPR.

2. Purpose and Scope

- 2.1. This Regulation lays down the terms according to which the INL processes personal data and guarantees its confidentiality, protection and security.
- 2.2. This Regulation applies to all Members of the INL Personnel and external entities processing personal data of behalf of INL.

3. Definitions

- (a) 'Controller': means the INL, which determines the purposes and means of the processing of Personal Data;
- (b) 'Data breach': a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (c) 'Data protection team': the team as established in Article 15;
- (d) 'GDPR': the 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).
- (e) 'Personal data': 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, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier;
- (f) 'Processor': a natural or legal person, agency or other entity which processes the personal data on behalf of the Controller;

- (g) 'Processing of personal data': any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (h) 'Pseudonymisation': 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- (i) 'Special categories of data': personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
- (j) 'Profiling': any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
- (k) 'Sub-processor': a natural or legal person, public authority, agency or other entity contracted by the Processor which processes personal data on behalf of the Controller.
- (l) 'CCTV': means fixed and domed cameras designed to capture and record images of individuals and property.

4. Principles

- 4.1. The processing of personal data shall be carried out and interpreted in accordance with the following principles:
 - (a) Lawfulness, fairness and transparency. The processing of personal data shall be carried out lawfully, fairly and in a transparent manner and in strict compliance with the right to privacy, as well as with the fundamental rights, freedoms and guarantees of data subjects;
 - (b) Purpose limitation. Personal data shall be collected for specified and explicit purposes and not further processed in a manner that is incompatible with those purposes;
 - (c) Data minimisation. Personal data shall be processed appropriately and limited to what is necessary in relation to the purposes for which they are processed;
 - (d) Accuracy. Personal data shall be accurate, where necessary, kept up to date;

- (e) Storage limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- (f) Integrity and Confidentiality. Personal data shall be processed in a manner that ensures its appropriate security, including the protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, ensuring in particular that:
 - (i) Personal data are only accessed by those who are duly authorised and need such access for their duties;
 - (ii) Informal data sharing is not permitted, being required that the access to personal data be formally requested in accordance with internally defined procedures;
 - (iii) Personal data will not be made available to unauthorized persons, either internally or externally;
 - (iv) Personal data are reviewed and updated regularly. Where it is found that certain personal data are outdated or are not necessary, they should be either erased or pseudonymised or not made available.

5. Rights of the data subject

5.1. Data subjects shall be entitled to the following rights:

- (a) Right of information. The data subject shall have the right of receiving from INL information about: the terms under which their personal data is processed when collected or, should the data not be obtained from the data subject himself, at the time of the first communication to that data subject. This information shall be provided in writing, including by electronic means, and if the data subject so requests.
- (b) Right of access. The data subject shall have the possibility to obtain from INL confirmation as to whether or not personal data concerning him or her are being processed, and, if that is the case, the possibility of accessing the personal data, as well as information on the purposes of the processing, categories of personal data concerned, recipients to whom the personal data have been or will be disclosed, the envisaged period for which the personal data will be stored, among others;
- (c) Right to rectification. The data subject shall have the possibility to obtain from INL, without undue delay, the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- (d) Right to withdraw consent. When the processing of personal data is based on consent of the data subject, the latter shall have the possibility to submit a request to INL in order to withdraw his or her consent at any time, and no

unfavourable consequences are applied to him or her that are not associated with the non-completion of the processing for which consent is withdrawn. Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;

- (e) Right to erasure. The data subject shall also have the possibility to ask INL for the erasure of his or her personal data and INL will, as a result of this request, erase the personal data unless there is a legal basis not dependent on the will of the data subject that justifies the respective processing;
- (f) Right to restriction of processing. The data subject shall have the possibility to ask and obtain from INL restriction on processing if the processing is unlawful, no longer necessary (in whole or in part) and/or if there is no legitimate interest of INL in the processing, or simply at the request of the data subject, subject to INL's analysis;
- (g) Right to data portability: the data subject may, upon request, receive the personal data concerning him or her, which he or she has provided to a controller in a structured, commonly used and machine-readable format and may request that such data be transmitted to another controller. This right may be exercised in cases where the processing is:
 - (i) based on consent; and
 - (ii) is carried out by automated means.

The data subject also has the right to have the personal data transmitted directly from one controller to another, if technically feasible.

- (h) Right to object. The data subject shall have the possibility to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, in particular where his data are processed for the direct marketing purposes.
 - (i) Right not to be subject to automated individual decisions. The data subject shall have the possibility to request not to be subject to any conclusions or decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- 5.2. INL shall respond to requests for information within two working days and shall provide details for further processing of such request.
- 5.3. INL shall provide data subjects, regarding the terms of processing of their data, the following information:
- (a) The contact details of the Data Protection Team;
 - (b) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
 - (c) If the processing of the data is based on legitimate interests, the legitimate interests pursued by the controller or by a third party;
 - (d) The recipients or categories of recipients of the personal data (if any);

- (e) The fact that the controller intends to transfer personal data outside the EU territory, namely third countries, and international organisations;
 - (f) The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (g) The existence of the possibility to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to exercise data portability;
 - (h) The existence of the possibility to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (i) Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
 - (j) The origin of the data and the categories of personal data concerned, in the case of indirect data collection;
 - (k) The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- 5.4. Personal data of deceased persons that are included in the Special Categories of Data, or pursuant the intimacy, image or data relating to communications, are within the scope of this Regulation.
- 5.5. The rights regarding personal data of deceased persons, specified in paragraph 5.1., namely, the rights of access, rectification and erasure, shall be exercised by their heirs.

6. Personal Data Processing Rules

- 6.1. Personal data are collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes. Data processing is only possible if and to the extent that at least one of the following applies:
- (a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - (b) Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
 - (c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
 - (d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- (e) Processing is necessary for the performance of a task carried out in public interest;
 - (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.
- 6.2. Specific conditions applicable to consent:
- (a) The consent of the data subject is any freely given, specific, informed and unambiguous indication of the data subject's will 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. For certain types of data processing, including but not limited to, Special Categories of Data and cross-border data transfers within the European Union, consent shall be explicit;
 - (b) Where processing is based on consent, the Controller shall be able to demonstrate that the data subject has consented on processing his or her personal data. To this end, it should be possible to identify the situation and method by which such consent was provided;
 - (c) Consent should cover all processing activities performed for the same purpose. In cases where the processing serves multiple purposes, consent should be given for each of these purposes, clearly distinguished from other matters, in an intelligible and easily accessible form, using clear and plain language;
 - (d) The data subject shall have the possibility of withdrawing his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;
 - (e) Where personal data are collected from a child under the age of 13, INL requires that those who have parental responsibility over the child give their consent or authorise the processing of personal data.
 - (f) Purposes for which INL processes Personal Data will be defined in the corresponding privacy statements.

7. Grounds for the processing of Special Categories of Data

- 7.1. INL will only process Special Categories of Data for the purpose of carrying out its legal and contractual obligations if the processing is necessary for the establishment, exercise or defence of legal claims, is necessary for reasons of pursuing public interest mission, providing preventive medicine or work services or for assessing the employee's working capacity or with the consent of the data subject.

8. CCTV

- 8.1. INL uses CCTV cameras to view and record individuals on its premises, which is operated with the purpose of ensuring the safety and security of INL Members of

the Personnel, visitors, assets and property, as well as information located or stored in its premises.

- 8.2. CCTV cameras located in the INL Cleanroom may also be streamed in real time through INL's internal communication channels.
- 8.3. CCTV cameras inside INL premises record only images, being sound capture prohibited.
- 8.4. CCTV cameras may only focus on the perimeters and access points, and also on spaces whose goods and equipment require special protection.
- 8.5. CCTV cameras cannot focus the following:
 - (a) public roads, neighbouring properties or any other places that are not exclusive premises of the INL, except as strictly necessary to cover access to facilities;
 - (b) coding area of ATM's or other ATM payments;
 - (c) areas reserved to Members of the Personnel, namely sanitary facilities, meal areas, bedrooms, locker rooms, gymnasium, rest rooms, nursery rooms, meeting and office rooms.
- 8.6. CCTV cameras placed at INL's premises are required to have warning and prominent signs, to alert individuals that their image may be recorded.
- 8.7. INL ensures that recorded images are only viewed and accessed by Members of the Personnel and authorised Contractors Personnel, who have received a specific training, and whose role requires them to have access to such Data.

9. Data Processing for research, scientific or statistical purposes

- 9.1. Data Processing for research, scientific or statistical purposes must respect the principle of data minimization and include the anonymization or pseudonymisation.
- 9.2. When the Personal Data are processed for research, scientific or statistical purposes, the rights of access, rectification, withdrawn consent, erasure and restriction of processing pursuant to Article 5. may be restricted, to the extent necessary, if the exercise of those rights seriously affects the aforementioned rights.

10. Transfer of personal data outside INL

- 10.1. INL may communicate personal data of the subjects to other entities, such as:
 - (a) Subcontractors, for the processing of data on behalf of the INL. In these cases, INL ensures that such processors provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the legal and regulatory requirements in force, including this Regulation, and ensures the protection of the rights of data subjects;

- (b) Third parties, where transfer of data is necessary for the fulfilment of any legal obligations or court orders, or for the satisfaction of requests from public or government authorities, such as the Tax Authority, Social Security, among others. In any of the situations mentioned above, INL takes all reasonable measures to guarantee the effective protection of the personal data that it processes.
- 10.2. Transfers of personal data outside the EU territory or to international organisations
- (a) In certain situations, INL may:
 - (i) transfer personal data to third countries (other than those belonging to the European Union or the European Economic Area), for which no adequacy decision has been issued regarding the level of protection of personal data under the GDPR;
 - (ii) transfer personal data to entities located in the European Union subject to the GDPR which consequently implies that INL complies with the security and compliance standards set out in the applicable legislation in order to be able to operate the mentioned data transfer.
 - (b) The data subjects shall have the possibility to request and obtain information about the measures taken by INL to guarantee the protection of personal data under the previous paragraph.

11. Confidentiality and security measures

- 11.1. The INL shall implement the appropriate technical and organisational measures to ensure a level of security adjusted to such risks, such as:
- (a) Pseudonymisation and encryption of personal data, where possible;
 - (b) The ability to ensure the continued confidentiality, integrity, availability and resilience of the processing systems and services;
 - (c) The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure secure processing.
- 11.2. INL Members of the Personnel who process personal data in the exercise of their duties are bound by professional secrecy, even after termination of their duties, under the terms best defined in the respective contracts concluded with INL and the applicable rules.
- 11.3. INL Members of the Personnel must also ensure that the data processing in question also complies with the provisions of this Regulation and other policies and instructions issued by INL in this matter.

12. Storage of Personal Data

- 12.1. The storage periods of personal data vary according to the purposes for which the data are processed by INL. The data are stored during the legal or contractually defined period of time or, in the absence of such period, for the period strictly necessary for the purposes for which the data were collected or are subsequently processed after which the data will be permanently erased.

13. Notification of Data Breaches

- 13.1. The INL will take the necessary measures to manage personal data breaches. When identifying that a personal data breach has occurred, the INL Members of the Personnel must:
- (a) Report the situation to their hierarchical superior as soon as they are aware of it and within a maximum period of one working day;
 - (b) Formalize, in writing, by filling the Record of Security Incidents regarding Personal Data. Such record shall at least include the following information:
 - (i) type of data breach;
 - (ii) who acknowledged the breach;
 - (iii) when was the breach acknowledged;
 - (iv) categories of personal data breached;
 - (v) number of data subjects potentially affected;
 - (vi) potential consequences of the personal data breach and their likelihood.
- 13.2. The Data Protection Team ('DPT') shall prepare a report of the personal data breach and notify it to the Director-General within three working days of becoming aware of it. The report shall, at least:
- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) describe the likely consequences of the personal data breach;
 - (c) describe the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

14. Data Protection Impact Assessment

- 14.1. Where a type of personal data processing to be carried out is likely to result in a high risk to the rights and freedoms of natural persons, the INL shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, in accordance with this Article.

- 14.2. The Members of the Personnel intending to carry out the processing of personal data shall seek advice of the Data Protection Team, who shall conduct the Data Protection Impact Assessment.
- 14.3. The Data Protection Impact Assessment ('DPIA') shall in particular be required in case of:
- (a) processing involving Special Categories of Data;
 - (b) processing involving tracking and individual's geo-localization or behaviour;
 - (c) processing involving the risk of physical harm of individuals;
 - (d) processing involving systematic monitoring;
 - (e) data processed on a large scale.
- 14.4. A Data Protection Impact Assessment shall not be required when the nature, scope, context and purposes are similar to processing for which a DPIA has already been carried out.

15. Data Protection Team

- 15.1. In order to ensure the implementation of this Regulation in the context of the INL structure, a Data Protection Team shall be established.
- 15.2. Composition. The Data Protection Team shall consist of at least five members appointed by the Director-General, representing the following organisational functions: Legal Service, Quality Systems Management, Business and Strategic Relations, Corporate Communication and Marketing, Information and Communication Systems.
- 15.3. The members of the Data Protection Team are subject to the obligation of confidentiality.
- 15.4. The DPT must act independently, impartially and solely in the interest of the INL.

16. Duties of the Data Protection Team

- 16.1. The DPT shall have preventive powers. In particular, it may:
- (a) inform and advise the Controller or the processor and the Members of the Personnel who carry out processing of their obligations pursuant to this Regulation;
 - (b) receive written complaints from data subjects;
 - (c) access the relevant files where personal data are processed;
 - (d) suggest investigations;
 - (e) order data controllers to restrict or discontinue processing;
 - (f) recommend to the Director-General any necessary actions in case of misuse of personal data; and
 - (g) provide advice where requested as regards the data protection impact assessment and monitor its performance.

17. Dispute Resolution

- 17.1. The INL shall co-operate in an amicable manner with a view to achieving the successful resolution of any disagreements or disputes arising in connection with this Regulation.
- 17.2. If however no settlement of any disagreement or dispute has been possible to achieve after the Institution and the INL reasonable endeavours to settle such disputes amicably within 30 (thirty) days of the beginning of the discussions, the matter shall be referred to and find a resolve by arbitration, under the Portuguese Law on Voluntary Arbitration (Law 63/2011, dated 14th December).
- 17.3. The number of arbitrators shall be 1 (one).
- 17.4. The arbitrator shall render his decisions in accordance with this Regulation.
- 17.5. The place of arbitration shall be the city of Braga (Portugal).
- 17.6. The language to be used in the arbitral proceedings shall be English.

18. Omissions and Revision

- 18.1. Any situations not foreseen under this Regulation shall be decided by the Director-General of the INL.
- 18.2. This Regulation may be revised and updated by the Director-General at regular intervals.

19. Entry into force

- 19.1. This Regulation shall enter into force on the date of its approval and it shall take effect retroactively as of 1 July 2019.