INCAS - Institutul Național de Cercetare-Dezvoltare Aerospațială "Elie Carafoli"
Bd. Iuliu Maniu nr. 220, Sector 6, Cod 061126, Bucureşti, ROMÂNIA
Tel.: (+40-21) 434 00 83; Fax: (+40-21) 434 00 82
e-mail: incas@incas.ro
www.incas.ro

Research Data Management Plan

1. Description of data

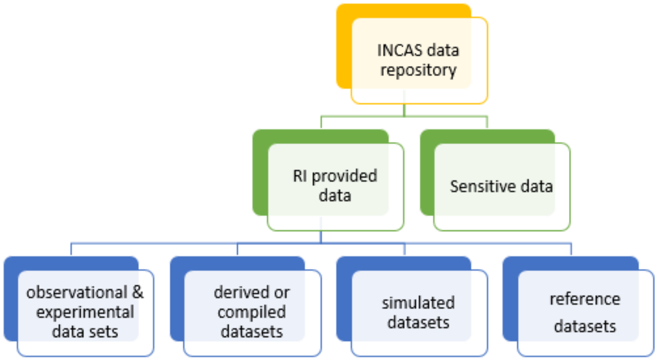
Data types produced by or associated with INCAS research infrastructures (RIs) are: experimental, observational, derived or compiled, simulation and reference (physical collections). Depending on the infrastructure used and the user's need, the data provided is given into specific data levels, starting from L0 (raw data), up to L2 (processed data). In terms of data formats, there are used several formats, as ASCII (text), binary, multimedia, models, software in-house codes, instrument specific, etc.

For each collected dataset (produced data depending on the exploration planning of each RI component), specific procedures for quality assurance and quality control (QA/QC) are used for detecting missing mandatory information, errors occurred during the transfer or reformatting, detection of duplicates and remaining outliers (spikes, out of scale data, vertical instabilities). In addition, internal QA/QC procedures are aligned with international standards applicable for each data type in order to assure a highly accurate data profiling. In accordance with recognized international adjustments of QA/QC procedures, research team leaders improve constantly the internal QA/QC procedures.

Some specific produced data is labelled as sensitive data, the access to it falling under the regulation of internal security policy of security.

2. Data Collection & storage

For each unit / facility of RI, there is applicable a specific methodology for data collection and management. Considering the specificity of each RI component, produced data are subject of QA/QC procedures, and then are stored into institutional repository. Access to this repository is granted for own personnel according to user-level security credentials. Sensitive data is stored on a secured and restrictive server, access being allowed only for team members and project partners (under specific non-disclosure agreement). Information are stored in an environment suited to its format and security classification to ensure its preservation from physical harm or degradation and its security from loss or unauthorised access.



For long term preservation of data, the data sets are collected or converted into standard or open formats for long-term accessibility. This step is important because it allows INCAS to: encourage further research branching from the original project/experiment, establish new collaborations, encourages the transparency and the improvement of research practice, reduce the cost for further data collection and increase the profile as a research output. Backup and security of data are also key elements in data collection and storage. Thus, the raw and processed data is backed up regularly and secured.

3. Data sharing & open data

On request, RI provided data can be shared and used by the scientists and members of academic community. For reasons of security, privacy and confidentiality, some datasets or information cannot be shared with external users. For all the results obtained with data provided by INCAS research infrastructures, published in scientific articles and not only, the authors must include the National Institute for Aerospace Research „Elie Carafoli" – INCAS, Bucharest in the acknowledgement section.

Considering the multidisciplinary of INCAS activities, different approaches will have to be considered for the data provided. Each type of data is accompanied by contextual information of documentation to provide the secondary user with any necessary details on the origin or manipulation of the data in order to prevent any misuse, misinterpretation or confusion.

4. Legal and ethical aspects

Sensitive data security level is increased by acquiring and handling only the minimum amount of sensitive data strictly needed for the research study. The Personally Identifiable Information (PII) is separate from all other data. Also, the sensitive data is encrypted by different types of encryption: device-level (whole-disk), cloud storage, folder-level, IT-administrated options.

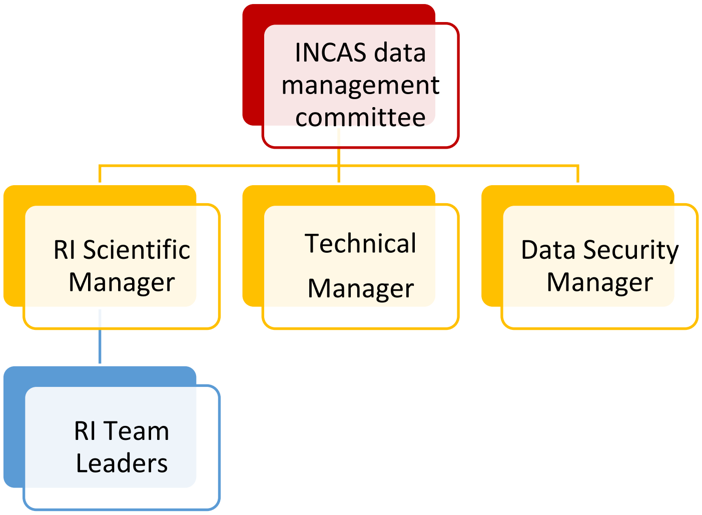
GDPR compliance is in conformity with Regulations (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

5. Agreements on rights of use and licence

In general, the ownership of the data is held by the institute, excepting the funded project where the intellectual property of the data and /or results is own by the financing authority (these aspects are clearly mentioned in the contract). Data generated within a research funded project / service provision contract are used to fulfil all the assumed commitments, and also contributing on cutting-edge science and technology niches development. The right to use the data for external users is given after obtaining INCAS approval (within formal request submitted to INCAS are included several aspects as description of the project, purpose of data usage, expected results, description of the project and commitment to acknowledge INCAS for shared data).

6. Data management responsibilities

At institutional level, the management of the data is ensured by a committee of 5 members with strong scientific, technical and security background. External users' access to data is given after the approval of this committee.



Scientific Committee could also give recommendation related to the use, access and management of RI provided data. In terms of dedicated resources for data management, each RI team leader supervise the collection and storage of data. Based on security department recommendations, IT and technical department ensures the support for a homogeneous data management.