DATA PROTECTION IN THE CONTEXT OF THE EVALUATION

Information related to data protection and the processing of personal data can be found in our privacy policy available here.

The section below provides some clarification on:

1) The Data Protection Agreement (DPA) that the expert is required to sign prior to the examination of any proposal.
2) The list of technical and organisational measures suggested to ensure the protection of personal data in the context of the evaluation mission.

As stated in our privacy policy, any question regarding these matters can be sent to privacy@frs-fnrs.be and we will make sure that we respond to such question without undue delay.

1. DATA PROTECTION AGREEMENT

The purpose of the Data Protection Agreement is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**").

The experts or members of scientific commissions and juries of the FNRS (the "**Expert**") fulfil scientific research missions (the "**Mission**") with the Fund for scientific research in the French-speaking Community of Belgium, the Fonds de la Recherche Scientifique – F.R.S.-FNRS (the "**FNRS**") and its specialised Associated Funds involving the processing and consultation of personal data.

In accordance with the GDPR, processing of personal data by the Expert on behalf of the FNRS shall be governed by a contract that is binding on the Expert with regard to the FNRS. The Data Protection Agreement sets out commitments of the FNRS and the Expert so that both parties also understand their responsibilities and liabilities, and contains the provisions of article 28 of the GDPR as interpreted by the European Data Protection Board in its opinion 14/2019 (i.e., subject matter of the processing in the Guide for reviewers, instructions of the FNRS, security measures, transfers of personal data, etc.), to ensure the security of the personal data processed by the Expert when performing the Mission (for e.g., when consulting personal data made available to the experts by the FNRS).

The FNRS and the Expert can sign the Data Protection Agreement electronically on the E-Space Platform[1].

[1] If you are entering into the Data Protection Agreement on behalf of the Expert, you warrant that (a) you have full legal authority to bind the Expert to the Data Protection Agreement, and (b) you agree, on behalf of the Expert, to the Data Protection Agreement. If you do not have the legal authority to bind the Expert, please do not sign the Data Protection Agreement and pass it on to the relevant representative.

In case of questions about the Data Protection Agreement or in regard to the processing of personal data on behalf of the FNRS in the context of the Mission, the Expert can contact the FNRS at all times via email at the following address: privacy@fnrs.be.

2. TECHNICAL AND ORGANISATIONAL MEASURES

The processing and consultation of personal data by the Expert should be operated solely on the F.R.S.-FNRS E-Space secure platform, using the personal login and password of the Expert.

The processing and consultation of personal data outside of the platform (for example, in case the data is downloaded from the platform) falls under the responsibility of the expert, solely. The expert therefore commits to take all reasonable measures to ensure the security and protection of the personal data. An illustrative list of such measures is presented below:

Technical and organizational measures suggested to be respected in the context of expertise missions conducted on behalf of the F.R.S-FNRS:

1. Technical measures

☐ Antivirus on all PCs/servers and regular updates
☐ Measures against loss of personal data and regular back-ups
☐ Systematic and automatic software updates
☐ Website with secure https connection
☐ Firewalls and authentication systems
☐ Physical security of servers (reception, locked room, authorisation of authorised personnel)
☐ Access system with a unique identifier (login) for each user and authentication mechanism to be put in place
☐ Configuration of new and existing hardware to reduce vulnerabilities
☐ Limiting access to personal data held in information systems
☐ Appropriate passwords (secure and regularly changed) and a process to detect any unauthorised access or abnormal use
☐ Encryption on the network and mobile devices (e.g. for sensitive data)
☐ Anti-malware defences
☐ Network intrusion detection or prevention system
☐ Wi-Fi protected by WPA2 encryption
☐ Logging and monitoring processes of user and system activity to identify and help prevent data breaches
☐ Control and management of removable media to prevent unauthorised disclosure, encryption, deletion, or destruction of personal data
☐ Secure storage devices to protect records, equipment and prevent loss, damage, theft or endangerment of personal data
☐ Other

2. Organizational measures

☐ Internal security policy (data breach scenario, staff arrival and departure procedure, ICT best practices, etc)
☐ Awareness-raising of staff and management involved in the processing of personal data
☐ Training of staff and management involved in the processing of personal data

☐ Appointment of a DPO or Data Manager (Team)
☐ Appointment of an Information Security Officer
☐ Internal organisation chart and clear division of labour
☐ Anonymisation/Pseudonymisation of data (e.g. sensitive data)
☐ Restriction and control of access to premises, equipment and data according to authorisation/function ("need-to-know")
☐ Prevention, detection and treatment of physical hazards (fire, water damage, etc.)
☐ Secure data deletion process (e.g. shredder, etc.)
☐ Recovery, disaster or contingency plan (continuity plan)
☐ Regular information security awareness training for all staff (and subcontractors)
☐ Other