PERSONAL DATA PROTECTION POLICY

Regulation (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 Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights

TABLE OF CONTENTS

The Managing Board of CONSORCIO CENTRO DE INVESTIGACIÓN BIOMÉDICA EN RED M.P. (hereinafter referred to as "CIBER"), within its framework of responsibility and in order to establish the general principles governing the processing of personal data at CIBER, hereby approves this Personal Data Protection Policy.

1. Purpose

The Personal Data Protection Policy establishes the guiding principles of CIBER regarding personal data protection and guarantees compliance with current legislation, and particularly with Regulation (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 (GDPR), and Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD).

2. Scope

The Personal Data Protection Policy is applicable to all CIBER units, the members of the technical office, the staff, and any individuals and entities related to CIBER.

3. Principles of Personal Data Processing

CIBER shall ensure that the principles of personal data processing are implemented *from the initial design* in all procedures involving personal data processing.

i. Lawfulness, Fairness and Transparency Principles

CIBER shall take any necessary measures to ensure that the processing of personal data is carried out in a lawful, fair and transparent manner. Personal data processing shall always be backed by a legal basis enabling it, and all individuals shall be notified of the purpose for which their personal data are processed using a clear, concise and easily accessible language. Within the scope of the research projects owned by CIBER, patient data shall be collected using clear and concise information, explaining the advantages and disadvantages of their involvement in a given research project. Personal data collection shall only be carried out after obtaining the consent of the subject taking part in the research project.

ii. Purpose Limitation Principle

CIBER shall develop any necessary internal procedures to ensure that personal data are processed for the explicit and lawful purpose for which they were collected. In no event shall data be processed in a manner incompatible with said purposes. Within the scope

of the research projects owned by CIBER, and pursuant to the seventeenth additional provision of LOPDGDD, the re-use of personal data for biomedical research purposes is acceptable, provided personal data are used for research purposes or areas related to the area to which the initial study pertains from a scientific perspective. Said re-use of data shall be carried out, if required, prior to obtaining the favourable opinion of the competent Research Ethics Committee.

iii. Data Minimisation Principle

CIBER shall process the strictly necessary amount of data related to the purposes for which they were collected. In a research setting, which inherently requires the processing of multiple types of personal data in order to achieve the required objective, personal data shall be processed at least in a pseudonymised form, together with a technical and functional division between the research team and the individuals in charge of maintaining the information which allows for re-identification.

iv. Accuracy Principle

CIBER shall adopt any internal procedures to update data, taking any reasonable measures in order to promptly remove or rectify any inaccurate personal data in relation to the purposes for which they are processed. In a research setting, one of the main objectives is to guarantee the integrity of personal data for them to be reliable in terms of coherence and truthfulness, ensuring that data collection is carried out lawfully and that the integrity of personal data is maintained throughout the whole process.

v. Conservation Period Limitation Principle

CIBER shall keep all personal data during the period of time necessary for the fulfilment of the personal data processing purposes; however, data may be retained for longer periods of time for archival purposes in the public interest, scientific research purposes and statistical purposes. Nevertheless, within the scope of the research projects owned by CIBER, participants shall be entitled to revoke their consent at any time, thus having control over their personal data at all times.

vi. Safety Principle

CIBER shall process data ensuring an appropriate level of safety by taking adequate technical and organisational measures preventing the unauthorised or unlawful processing of personal data, as well as any loss, destruction or accidental damage to them.

vii. Proactive Responsibility Principle

CIBER shall be responsible for compliance with the Principles established in this Policy and with current legislation, and it shall be able to provide proof of compliance with those measures by means of the following actions:

- CIBER has appointed a Data Protection Officer and is implementing all the necessary measures to ensure that its participation is carried out correctly and promptly in any issues regarding personal data protection.
- CIBER has created a Registry of data processing activities carried out under its responsibility, which was made public by electronic means.
- CIBER has carried out a risk assessment of the data processing activities performed by CIBER in order to determine the appropriate technical and organisational measures to be adopted.
- CIBER is carrying out Data Protection Impact Assessments for the research projects owned by the organisation.
- CIBER has designed and implemented an internal procedure in order to manage any incidents caused by the accidental or unlawful destruction, loss or alteration of personal data, or the unauthorised access to, or sharing of, said data. Such incidents shall be documented and measures shall be taken to minimise their negative effects.
- CIBER has planned training actions regarding personal data protection.
- CIBER carries out verification audits annually in order to ensure that the measures and procedures adopted by CIBER regarding personal data are not only nominal but also functional and applied on the ground.

viii. Engagement of Data Processing Officers

CIBER has internal procedures in place in order to ensure that, prior to hiring the services of a provider who may have access to personal data under CIBER's responsibility, only

providers offering a sufficient level of assurance regarding the fulfilment of current data protection regulations, the adoption of adequate technical and organisational measures, and the guarantee of the rights of data subjects are engaged.

ix. Rights of Data Subjects

CIBER has drafted internal procedures necessary for data subjects to exercise their rights of access, rectification, deletion, limitation of processing activities, portability and objection.

This Personal Data Protection Policy was approved by Mr. Manuel Sánchez Delgado, Director of CIBER, in Madrid on 9 March 2020.