## Annex XIII

## Data Protection Compliance Declaration

For the provision of medical services under FWC 09/2018/OP/EITPROC

Each tenderer / consortium members / subcontractor must sign this form.

*(Complete or delete the parts in grey italics in parentheses)*

[Choose options for parts in grey between square brackets]

The undersigned *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*:

* in [his][her] own name *(for a natural person)*

or

* representing the following legal person: *(only if the economic operator is a legal person)*

Full official name:

Official legal form:

Full official address:

VAT registration number:

1. declares that [the above-mentioned legal person][he][she] in his/her role as ‘processor’ within the meaning of Article 4(2) and (8) of the General Data Protection Regulation (GDPR, Regulation (EU) 2016/697[[1]](#footnote-2)):
2. shall process all personal data[[2]](#footnote-3) in compliance with the GDPR (and any respective implementing act under Hungarian law, if applicable);
3. may only process personal data for the purposes of Framework Contract 09/2018/OP/EITPROC (hereafter referred to as “Contract”). Data shall not be reused for a purpose incompatible with the original purpose;
4. may act only under the supervision of the EIT and CEPOL (hereafter referred to as the “Agencies”), in particular with regard to the purposes of the processing of personal data, the categories of data which may be processed, the recipients of the data and the means by which the data subject may exercise his/her rights;
5. shall solely transfer personal data to third parties according to specific instructions and appropriate security safeguards being implemented to avoid unauthorised processing and disclosure;
6. shall grant its personnel access to the data only to the extent strictly necessary for the performance and management of the services under the Contract;
7. guarantees, that any of its staff members processing medical data covered by the Contract have been instructed to comply with all applicable data protection laws, and have signed a declaration of confidentiality if the respective staff member is not a health professional subject to the obligation of professional secrecy or is not subject to an equivalent obligation of secrecy under the applicable laws;
8. shall grant to the Agencies and the European Data Protection Supervisor at any time (during the term of the Contract) access to all the premises where personal data is processed under the Contract in order to monitor the compliance with the present Data Protection Compliance Declaration;
9. guarantees, that no personal data under the Contract will be processed outside the premises of the medical centre without the prior written consent of the concerned Agency;
10. guarantees, that no personal data under the Contract will be processed outside Member States of the European Union or the European Economic Area[[3]](#footnote-4) without the prior written consent of the concerned Agency;
11. guarantees, that personal data are kept for no longer than is necessary for the purposes for which they were collected, in accordance with the GDPR (and any respective implementing act under Hungarian law, if applicable).
12. declares that [the above-mentioned legal person][he][she] has undertaken and continuous to undertake to adopt appropriate technical and organisational security measures having regard to the risks inherent in the processing and to the nature of the personal data concerned in order to
13. prevent any unauthorised person from gaining access to computer systems processing personal data, and especially:
14. unauthorised reading, copying, alteration or removal of storage media;
15. unauthorised data input, as well as any unauthorised disclosure, alteration or erasure of stored personal data;
16. unauthorised use of data-processing systems by means of data transmission facilities;
17. ensure that authorised users of a data-processing system can access only the personal data to which their access right refers;
18. record which personal data have been communicated, when and to whom;
19. ensure that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the Agencies;
20. ensure that, during communication of personal data and transport of storage media, the data cannot be read, copied or erased without authorisation;
21. design its organisational structure in such a way that it meets data protection requirements.

The technical and organisational security measures undertaken by the service provider with regard to the aforementioned Section 2 are as follows[[4]](#footnote-5):

*(…)*

Full name Date Signature

1. General Data Protection Regulation (GDPR): 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, OJ L OJ L 119, 4.5.2016, p. 1–88. [↑](#footnote-ref-2)
2. For the definition of the term ‘personal data’ see Article 4(1) of the GDPR. [↑](#footnote-ref-3)
3. This should also include the use of cloud computing infrastructure. [↑](#footnote-ref-4)
4. Short description of technical and organisational security measures should be provided (or as alternative: Data/IT Security Concept or audit report should be enclosed). [↑](#footnote-ref-5)