Data Protection Addendum to the ICTSS Agreement

HEAnet provide services to the HEAnet Clients, in accordance with a Client Services Agreement.

HEAnet and the HEAnet client have concluded an Agreement for ICT Security Services (hereafter, the Agreement), to which this Data Protection Addendum is incorporated by reference.

Whereas in this context, each HEAnet Client is the 'Data Controller' (hereafter Controller or Client) and HEAnet acts as 'Data Processor' with respect to personal data.

This Addendum outlines provisions for the protection of personal data related to the Services as required by the General Data Protection Regulation and is supplemental to the ICT Security Services Agreement.

The Parties agree as follows:

1. Definitions

Unless otherwise defined in the Agreement, all capitalised terms used in this Addendum will have the meanings given to them below. If any definitions set forth herein or in the Agreement conflict with statutory definitions provided in any applicable Data Protection Law, the definition in the Data Protection Law shall control:

"**Affiliate**" means any entity that, directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with a party or any direct or indirect parent company of a party. As used in this definition, "control" means the ability to direct or cause the direction of the management or policies of an entity, whether directly or indirectly through ownership, contract or otherwise.

"**Applicable EU Legislation**" means the General Data Protection 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 ("GDPR") and, (iii) any applicable EU Member State Legislation.

"**Controlle**r" means the party which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Data Protection Law(s)**" means the Applicable EU Legislation and any other data protection laws which may be applicable to the Personal Data Processed under the Agreement.

"**EEA**" means the European Economic Area.

"Supplier" means the suppliers and service providers as defined in the Agreement and as otherwise notified or agreed from time to time.

"**Personal Data**" means any information related to any identified or identifiable natural person (the "**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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The Data Subjects herein may be Data Controller employees, contractors, end users, customers, customers' end users or employees, and/or other third parties.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"**Process**" means 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the party that Processes Personal Data on behalf of the Controller and, for purposes of this Schedule, means HEAnet and any HEAnet Affiliate.

"**Services**" means the Services as described in the Agreement and any HEAnet Service Description documents as amended or updated from time to time.

2. Compliance with Laws

Each Party will comply with the Data Protection Laws as applicable to it. To the extent required by any Data Protection Law(s), the Parties agree to negotiate in good faith and execute any such additional, supplemental or revised documents pertaining to the Processing of Personal Data as reasonably necessary for the provision of Services under the Agreement.

3. Data Processing

HEAnet shall process Personal Data only on the instruction of the Data Controller unless processing is required by applicable Data Protection Laws. Each of the Data Controller and its relevant Affiliates instruct HEAnet and any additional Processors specified in the annexures hereto as amended from time to time to process the personal data set out in the annexures for the purpose of providing the Services described in the Agreement.

The annexures set out certain information regarding the Suppliers processing of Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws).

HEAnet may refer proposed amendment to any of the annexures or refer additional annexures for additional Services to the Data Controller from time to time such that the Data Controller may determine

the means and purpose of processing necessary to meet the current or future requirements of the Data Controller and the delivery of present or future Services.

HEAnet will refer amendment to or additional annexures to the Data Protection Addendum. Within ten (10) days of receipt, the Data Controller shall accept, object, vary or reject the proposed amendment, failing which the proposed amendment will be deemed to be properly made and become an operable part of this Data Protection Addendum.

4. HEANET Employees/Agents

HEAnet will restrict access to Personal Data to those employees and agents who require such access to perform the Agreement and will ensure that those employees/agents are or shall be: i) directed to keep such Personal Data confidential; and, ii) subject to written confidentiality obligations consistent with this Schedule and applicable Data Protection Laws. HEAnet shall procure that the terms of this clause are reflected in the data protection agreements with the Supplier.

5. Data Subject Rights and Controller Assistance

HEAnet shall notify the Data Controller of any request it receives from a Data Subject(s) or any other party in regard to Personal Data of the Data Controller. HEAnet will not respond to such requests except on the instruction of the Data Controller or as required by applicable Data Protection Laws. HEAnet will reasonably assist the Data Controller with obligations it may have to comply with Data Protection Laws.

6. Technical and Organizational Security Measures

HEAnet shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of any processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk.

7. Audit of Technical and Organizational Security Measures

Upon the request of the Data Controller, HEAnet agrees to make available all information necessary to demonstrate compliance with data protection obligations implemented as part of the Services applicable under the Agreement. HEAnet will allow for and contribute to audits, including inspections, by the Data Controller or an auditor mandated by the Controller, to the extent necessary to demonstrate compliance with this DPA and Article 28 GDPR. Such audits shall be at the Controller's expense and may be satisfied through the provision of relevant third-party certifications or audit reports made available by HEAnet.

8. Location of Processing

All processing of personal data shall be within the EEA unless otherwise specified to the HEAnet client.

9. Data Breach Notification and Remediation

HEAnet will notify the Data Controller without undue delay if there has been a Personal Data Breach involving Personal Data. HEAnet shall provide the Data Controller all reasonably required support and cooperation necessary to enable the Data Controller to comply with its legal obligations in case of a Personal Data Breach.

The Data Controller will defend, indemnify and hold harmless HEAnet and its agents, against any and all third-party claims, actions and expenses including fines or penalties, arising from or relating to Personal Data Breach caused by the Data Controller breach of the terms of the Data Protection Addendum and/or with respect to its use and that of its end-users.

10. Appointment of Additional Processors

HEAnet are generally authorised to appoint additional processors (including to authorise the appointment of additional processors on receipt of notice from Suppliers) where it deems reasonably necessary to support delivery of services and shall not be obliged to seek the consent of the Data Controller before it engages third party providers as Processors of Personal Data.

For new Processors appointed, HEANET shall, where applicable, use reasonable endeavours to provide the Data Controller Agreement notice of up to ten days (10) days prior to allowing a Processor access to Personal Data. The Data Controller may object to a new Processor within the period of notice in which case HEAnet will use commercially reasonable efforts to change the Services (including to engage with the Suppliers) to ensure that Personal Data of the Data Controller is not processed by the new Processor in question.

HEAnet shall seek appropriate contractual obligations in writing with the Suppliers and/or any additional Processor directly appointed by HEAnet on terms substantially similar to this Addendum. HEAnet shall remain liable, in accordance with Article 28(4) GDPR, for ensuring that any Processor it appoints complies with its data protection obligations under that Article"

11. Compliance and Return or Deletion of Personal Data

HEAnet shall monitor compliance with these terms and ensure that its personnel are suitably trained with regard to processing Personal Data. On receipt of the written request of the Data Controller following cessation of Services HEAnet shall delete or return, as specified by the Data Controller, Personal Data held by HEAnet within a reasonable period of time unless applicable EU or EU member state law prevents it from returning or destroying all or part of the Relevant Data disclosed.

12. Order of Precedence

If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

This Annex 1 includes certain details of the Processing of Personal Data.

1.Subject matter and duration of the Processing of Company Personal Data.

The subject matter and duration of the Processing of the Personal Data are set out in the Agreement and this DPA.

2.The nature and purpose of the Processing of Personal Data.

Processing of Personal Data as reasonably required in the performance of the Services and for statistical purposes.

3.The types of Personal Data to be Processed

Email address, first and second name, job title, employing organisation.

4. The categories of Data Subject to whom the Personal Data relates

Staff and other personnel

5. The obligations and rights of HEAnet and HEAnet clients

The obligations and rights of HEAnet and HEAnet clients are set out in the Agreement and this DPA.

6.The physical location of Personal Data Processing activities by Processor under the Agreement

HEAnet servers in Dublin, Ireland.

8. List Sub-Processors that will Process HEAnet or Data Controller personal data and include the location(s) and purpose of such sub-processing activities.

Processor: SendGrid (now Twilio Inc)
Location: NL
Purpose: mail service to email large volume phishing emails to the email servers of the client institution

Processor: Leaseweb Global BV
Location: NL
Purpose: encrypted virtual disk storage for HEAnet leased virtual server, server is used to send phishing emails

Processor: MetaCompliance Ireland Limited
Location: United Kingdom
Denmark
Portugal
Germany
Ireland (MetaCompliance Group, Microsoft Azure, Amazon Web Services)
Holland (Microsoft Azure)
Purpose: Cyber Security eLearning courses for client institutions.