This project has received funding from the European Union's Horizon 2020 research and innovation Programme under grant agreement No 645852

EU Grant Agreement number: 645852

Project acronym: DIGIWHIST

Project title: The Digital Whistleblower: Fiscal Transparency, Risk Assessment and the Impact of Good Governance Policies Assessed

Work Package 6: Sustainability

Title of deliverable: 6.1 Collaboration agreement among consortium partners

Due date of deliverable: 28 February 2018
Actual submission date: 28 February 2018

Author: Aram Khaghaghordyan

Organization name of lead beneficiary for this deliverable: Hertie School of Governance

Dissemination Level		
PU	Public	☑
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
Co	Confidential, only for members of the consortium (including the Commission Services)	

Memorandum of Understanding on the Sustainability of the EU Horizon 2020 DIGIWHIST project (MoU)

between

THE CHANCELLOR, MASTERS AND SCHOLARS OF THE UNIVERSITY OF CAMBRIDGE (UCAM)
TRINITY LANE, CAMBRIDGE CB2 1TN, UNITED KINGDOM,

UNIVERSITA CATTOLICA DEL SACRO CUORE (UCSC)
LARGO AGOSTINO GEMELLI 1, MILANO 20123, ITALY

GOVERNMENT TRANSPARENCY INSTITUTE (GTI)
FUTÁR u. 48, KECSKEMÉT 6000, HUNGARY,

DATLAB SRO (DATLAB)
THUNOVSKA 179/12, PRAHA 11800, CZECH REPUBLIC,

OPEN KNOWLEDGE FOUNDATION DEUTSCHLAND (OKFDE)
Singerstr. 109, BERLIN 10179, GERMANY,

and

HERTIE SCHOOL OF GOVERNANCE GGMBH (HSOG)
FRIEDRICHSTRASSE 180, BERLIN 10117, GERMANY.

Memorandum of Understanding
on the Sustainability of the EU Horizon 2020 DIGIWHIST project (MoU)

Section 1: Introduction

1.1. In the framework of the Horizon 2020 Research Programme a consortium of six partner organizations that signed this MoU (hereinafter Consortium) worked on DIGIWHIST project (full title: "The Digital Whistleblower. Fiscal Transparency, Risk Assessment and Impact of Good Governance Policies Assessed" Grant Agreement n° 645852) from 01 March 2015 until 28 February 2018. The Consortium has conducted three years of research and tool development with the aim of increasing transparency and accountability in the field of public procurement in 35 jurisdictions (28 EU member states, Norway, the European Commission, Iceland, Switzerland, Serbia, Georgia and Armenia). The research results led to the creation of Data Collection Infrastructure and diverse tools (Opentender, EuroPAM, MET) for different actors and stakeholders interested in fair, transparent and efficient public procurement enabling the public to better monitor tenders and procedures.

Section 2: Objective

2.1. The first objective of this MoU is to fulfil the DIGIWHIST grant agreement and create collaboration agreement among consortium partners in particular its clauses on maintaining the data collection infrastructure and the tools created as part of DIGIWHIST project (DIGIWHIST tools).

2.2. The second objective of this MoU is to create a DIGIWHIST network on public procurement (hereinafter DIGIWHIST network) that will be based on the work conducted by DIGIWHIST project on Opentender.eu and will take into account its research results and important of continuing its sustainability. The DIGIWHIST network will include NGOs and stakeholders active in the field of public procurement.

Section 3: DIGIWHIST Data Collection Infrastructure and tools

3.1. **DIGIWHIST website** is a platform where all research results of the DIGIWHIST project are published. DIGIWHIST website is available at www.digiwhist.eu. During the project duration it was managed by the HSOG. After the project expires it will be maintained by HSOG while editing rights are also retained by DIGIWHIST partners to pursue updates in line with DIGIWHIST goals.

3.1. **Making Public Tenders More Transparent (Opentender,** available on www.opentender.eu**)** is a platform that allows to search and analyze tender-level data from 33 European jurisdictions (28 EU member states, Norway, the European Commission, Iceland, Switzerland, and Georgia) either by national portal or by exploring all available data at once. Opentender allows for selecting between different ways of interacting with the data, enabling users to compare different tenders as well as identify red flags specific to those tenders based on DIGIWHIST indicators. Opentender is ran by GTI (server hosting and domain) with DATLAB responsible for portal development, data collection and dissemination on behalf of GTI. During the project duration it was managed by OKFDE. After the project expires it will be transferred to GTI.

3.2. **European Public Accountability Mechanisms (EuroPAM)** is a data collection effort that produces assessments of in-law efforts across 35 European jurisdictions ((28 EU member states, Norway, the European Commission, Iceland, Switzerland, Serbia, Georgia and Armenia). EuroPAM allows the users to compare and visualize legal and regulatory norms in the fields of conflict of interest, public procurement, financial disclosure, party financing and freedom of information. EuroPAM is managed by HSOG and is available on www.euroPAM.eu.

3.3. **Monitoring European Tenders (MET)** - is a risk assessment software for public authorities to assess the degree of integrity of European public procurement procedures. MET is mainly addressed to public officials, who will be able to monitor tendering risks weighting indicators based on the importance they attribute to them relatively to their specific countries. MET allows to explore data searching by country, actor (company or contracting authority) and specific tender. MET provides an overview on the level of transparency and administrative capacity referred to specific tenders. MET is managed by Transcrime, the joint research center on transnational crime of UCSC and is available on www.monitoringeutenders.eu.

Section 4: Partner roles

4.1. **UCAM** will be in charge of overall promotion and support of the future DIGIWHIST network such as ethics advice on any future development and the continuation of mf436@cam.ac.uk as the main UCAM contact point (Mihály Fazekas to reply to queries).

4.2. **UCSC**, and in particular Transcrime, will be in charge of maintaining MET, as well as outreach and engagement of its potential users.

4.3. **GTI** will be responsible for overall project coordination on Opentender portal, running the servers for data and portals, indicators and analytics work, outreach and policy impact activities.

4.4. **DATLAB** will be responsible for programming work for the Opentender portal, keeping data collection and database building, running in line with DIGIWHIST standards.

4.5. **OKFDE** will serve as a chair for the newly created DIGIWHIST network, as well as participate in the outreach and engagement of potential users of the portals, scope user needs and gauge interests for collaborations.

4.6. **HSOG** will be in charge of maintaining and updating EuroPAM as well as outreach and engagement of its potential users.

Section 5: Data processing and protection for Opentender

5.1. DIGIWHIST Consortium members in charge of Opentender are GTI and DATLAB. GTI will become the data controller and DATLAB the data processor for any data used or accessed and GTI will be a nominated party to be the lead institution for responding to communications with data subjects.

5.2. Consortium members in charge of Opentender shall establish the security for data processing in accordance with Article 28 Paragraph 3 Point c, and Article 32 General Data Protection Regulation (GDPR) in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account [Details in Appendix 1: The Technical and Organisational Measures].

5.3. The Appendix 1: Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Consortium members to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

Section 6: Collaboration

6.1. Consortium partners will coordinate their efforts to build a DIGIWHIST network of NGOs and other stakeholders. Consortium partners will strive to apply for projects to make DIGIWHIST data collection infrastructure and tools sustainable.

6.2. Consortium partners will promote DIGIWHIST tools and policy recommendations to civil society and governments. Depending on the available funding Consortium partners will organise training on DIGIWHIST tools, data and best practices.

Section 7: Costs

7.1. Each Consortium partner will cover the costs arising with their own roles, as described by this MoU. The consortium partners shall not charge each other any costs under this MoU.

Section 8: Duration

8.1. This MoU is limited in time for the total of three years. It will enter into force on 01 March 2018 and cease on 28 February 2021 without notice. After the expiration of the MoU, partners can decide to agree on extending it further.

Section 9: Final provisions

9.1. This MoU has been drawn up in six copies. Each party shall receive one copy.

Appendix 1. Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control

No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems

- Electronic Access Control

No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media

- Internal Access Control (permissions for user rights of access to and amendment of data)

No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events

- Isolation Control

The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control

No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- Data Entry Control

Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management.

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control

Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning

- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control

No third party data processing as per Article 28 GDPR without corresponding instructions from the Consortium members in charge of Opentender, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

5. Responding to queries and complaints

Queries and requests received through the official opentender contact email would be received and evaluated by GTI. If the request potentially implies changes to data displayed at the Opentender portal, GTI will assess the merits of the query, its legal foundation and, if necessary, request Datlab to implement one of the below 3 types of actions on the tenders denoted in the query (based on Opentender tender ID in order to avoid any confusion about records to be impacted):

a) remove the denoted tenders in pursuance of the right to be forgotten;

b) remove performance indicators in the denoted tenders in pursuance of avoiding defamation;

c) correct a particular data field obtained from the official government source for the denoted tenders (correction possible at the next data update iteration).