EUROPEAN COMMISSION

MEETING BY VIDEOCONFERENCE ON THE HOSTING OF ECI ONLINE COLLECTION SYSTEMS BY THE EUROPEAN COMMISSION

8 August 2012

SUMMARY REPORT

PARTICIPANTS

Brussels (European Commission):

Declan Declan Deasy (Chair), Francisco Gimeno, Ivan Marusich, Marc Feidt (Informatics DG - DIGIT)

Manuel Szapiro, Charlotte Rive (Secretariat General – Institutional team G4),

Guido Vervaet, Peter Flack (DG Human Resources and Security – Security Directorate)

Paris: Vincent Chauvet (Single Communication Tariff Act)

Rome: Michele Trotta (Uno di Noi)

Italy: Carmelo Floridia (Uno di Noi)

Salzburg (via skype): Markus Gastinger (Fraternité 2020)

France (via skype) : Philippe Cayla (Let me vote)

1. PURPOSE OF THE MEETING, INTRODUCTION AND EXPECTATIONS FROM PARTICIPANTS

European Commission (EC) stressed its commitment to help the organisers beyond what the regulation requires. This first meeting would take them through the main steps and calendar.

Expectations from the organisers:

- to understand the progress and for one organiser who mentioned the related lack of funding, get access to a user friendly system.

- to have some information about the cost, the procedure and the timeline for the service proposed by the Commission.

- to understand what is required from their side, in particular for the Risk Analysis.

PROCESS AND RESPONSIBILITIES

EC recalled its legal obligations (to provide a register for European Citizen's Initiatives, to develop an Open Source Software for the collections of signatories and to guide the Member States for the certification process) which have been fulfilled and the responsibilities of the organisers (notification to data protection authorities, installing the software, submitting relevant documents for certification, collecting the statements of support).

In this teething stage, EC will support the organisers of already registered initiatives so they can fulfil their tasks. EC will in particular help them to:

- install their system for the Online Collection on a platform in the EC Datacentre

- notify the Data protection authorities (if help is needed)

- request the certification for the online system

- as mentioned in the 12 July letter to the organisers, the period for the collection of statements of support is also being extended

The EC confirmed that this Service will be free of charge and no additional fee will be requested when asking the certification to the Luxemburgish authorities.

2. STAY OF THE PLAY

EC explained the work accomplished so far: setting up the technical platform compliant with the Technical requirements, contact with Luxemburgish authorities in order to facilitate the subsequent certification process and elaboration of the first set of documents required for certification: Business Impact analysis, Security Scope, Risk Analysis (including threads and vulnerabilities) and Risk treatment plan.

3. PROCESS, DOCUMENTS AND ROLES

PROCESS

EC recalled what the organisers needed to do in accordance with the ECI Regulation (irrespective of the system they use for the hosting environment)

EC explained notably the difference between the formality of notification to the data protection authorities and the Certification of the online system.

Organisers need to notify the Data protection authority before collecting personal data. EC recalled that the notification needed to be made to the data protection authority of the country of residence of the 2 (or 3) organisers responsible for the

collection system. Further information on the contacts can be found on: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm (also accessible from the ECI register). Further information on notification requirements on: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2006-07-03-vademecum.doc

Certification of the Online system is requested to the competent authority of the country where the data is store (In the case of the Commission platform, the data is stored in Luxembourg). EC explained that, to obtain certification, the organisers need to comply with Security requirements and need to accept the residual risk. As explained below, the Commission will assist the organisers in the preparation of these documents.

DOCUMENTS

EC summarized the documentation that the organisers need to provide when asking for the certification: Risk Analysis, Risk treatment plan and Residual risk sign-off.

EC committed to help the organisers with a check list and guidance to complete those documents.

Main risks foreseen by EC for the organisers themselves are:

1. Not being able to administer the site during the complete collection period.

2. Loss/disclosure of the private key used to decrypt private data.

3. Management and transfer of large number (possible more than 1 million) of personal data records in the local organiser system.

EC will prepare the equivalent risk management documents for the software and infrastructure.

ROLES AND RESPONSIBILITIES

A hosting agreement document is under preparation. In this document the roles and responsibilities for the EC and the organiser are clearly defined. This document will be circulated and explained to the organisers. It is based on standard Host Provider Service Level Agreement and includes elements related to the service provided by the Commission and Security requirements to be complied with. A copy of this document should be handed over to the Luxemburgish authorities when asking for the certification.

The EC also confirmed that the organisers will not be responsible for checking the logs of the system.

An organiser also asked if a brand new laptop was needed for administrating the Online Collection System. EC answered that it is not required, but a secure environment is necessary. EU will help organisers to prepare such an environment.

4. TIMELINE

The organisers need to proceed with the notification to the (two) relevant data protection authorities (see above), with the help of the Commission whenever needed. This should be done before the formal request for certification is made to the Luxemburgish authority.

EC plans to have completed the host infrastructure and all assessment documents needed for certification by 7 of September.

Organisers need to complete their Risk Assessment, with the Commission's assistance. Based on it, they could request the certification of their system from **10 of September**.

As the certification process takes 1 month, their system could be open to collect data in the week of **15 of October**.

5. CLOSING REMARKS

EC urged the organisers who have not done so, to contact their data protection authorities and start working on the risk assessment for their own device.

This process will require bi-lateral meetings to work on the Risk Assessment/Risk Treatment Plan, Host agreement … EC is available for bilateral meetings, will provide guidance for completing the Risk Assessment, will guide the organisers in their notification to Data protection authorities and will provide the required training in the Online System.

The SG-ECI@ec.europa.eu remains the single entry point of contact for the organisers. From there, the organisers may be directed to the responsible people in the Commission.

A follow-up meeting with the organisers of all registered initiatives will be organised at the end of August.

A third meeting will take place before the expected date for launching the request for the certification (10 of September).

Finally, this summary report will be sent to all contact points (those participating in the meeting and those who were unable to participate) of initiatives having expressed an interest in the Commission's platform.

SUMMARY OF THE SERVICES EXCEPTIONALLY OFFERED BY THE EUROPEAN COMMISSION TO ORGANIZERS OF THE FIRST REGISTERED INITIATIVES

1. Host their system for the Online Collection on a platform in the EC Datacentre.

2. Preparation of all documents related to hosting environment for certification by Luxembourgish Authorities.

3. Advice on how to draft the organiser's Risk Management documentation.

4. Help the organisers on any other technical issue related to their certification request for their Online system.

5. Help the organisers in their notification to the Data protection authorities, if needed.

6. Train the organisers in the operation of OCS

7. Provide personalised assistance/guidance to the organisers