Terms of Reference for ENISA's personal data security in small and medium organizations stakeholders group

1 Background

ENISA has been working for several years to support the improvement of information security and data protection capabilities in small and medium organizations in Europe (SMOs). Within this line of work, ENISA launched in 2015 a project aimed to increase the intake of ICT security and data protection standards in European SMEs. One of the main findings of the project was the perceived lack of existing guidance regarding how to protect personal data in small and medium organizations. Indeed, SMOs are becoming increasingly concerned in Europe on protecting appropriately their clients and/or users information. However, deciding the appropriate security measures to implement, customized to the organization existing risk environment, is not trivial for small and medium organizations.

Based on the existing need for guidance in the area, the Agency has undertaken in 2016 an activity with the objective of developing: "A framework on appropriate security measures for the processing of personal data in small and medium organizations". The project output will consist of a series of handbooks, targeted to support SMOs in the selection of appropriate controls to protect personal data based on the assessed level of risk. The documents will cover the following areas:

- Guidelines for risk assessment on the processing of personal data.
- Guidelines for appropriate organizational security measures for the processing of personal data.
- Guidelines for appropriate technical security measures for the processing of personal data.
- Use cases that will demonstrate how to apply the proposed guidelines.

2 Objectives of the group

ENISA would like to engage a group of advisors, in order to gather valuable input from its target audience, which will help improve the quality of the recommendations. Members of the advisors' group are expected to validate the framework by providing their feedback regarding:

- The usability of the framework from a practitioner perspective.
- The applicability of the framework to their organization.
- Future possible improvements.

Once the group has been established, the Agency might further invite its members to participate in other projects of a similar nature in the following years. In such a case, the scope of the contribution would be of a similar nature (testing methodologies, frameworks, studies and/or tools in the area of improving security and privacy for small and medium organizations).

3 Selection of the members of the group

Members of the personal data security in SMOs advisory group will be appointed on an individual capacity. In order to match the profile of expected users of the framework, they should preferably be employed as information security officers and/or data protection officers in small and medium organizations.

The selection of members will be based on including expertise from different types of organizations:

- Small (from 10 to 50 employees) or medium organizations (from 50 to 250 employees).
- From a public, private or non-profit nature.
- From different activity sectors: health (e.g. a clinic), social (e.g. a school), professional services (e.g. a legal office), retail (e.g. a supermarket), etc.

Additionally, selection will aim to achieve a balanced geographical and gender representation.

4 Approach / Working Methods

The main means of interaction of the group will be online tools (web conferencing and electronic mails). The contribution of each member of the group is roughly estimated with ca. 2 person days per year. This engagement does not include the time required for a potential physical meeting.

Participation the group is non-remunerated by ENISA. In case attendance to a physical meeting is required, the Agency might cover the travelling costs of the members of the group (provided certain conditions are met).

Group members will be acknowledged in the ENISA reports.

5 Data Protection

Personal data of participants in the group will be processed in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

The members of group are subject to a requirement of confidentiality on the internal discussions and draft documents circulated to the group.

6 Expression of Interest

If you are interested in participating in the group, please send a short CV, and a short statement on your motivation to join the group, to the Information Security and Data Protection Unit of ENISA: isdp@enisa.europa.eu

Please express your interest before March 31st 2016.