Draft ID: cd66d607-c7e9-40a2-ab2d-96664673619e
Date: 04/01/2023 08:26:54

2022 ENISA Survey regarding the stakeholders' trust

Fields marked with * are mandatory.

INTRODUCTION TO THE SURVEY

Dear participant,

One of the core objectives of ENISA is to contribute to the development of secure digital solutions and, thereby, to increase trust in digital solutions among European businesses and citizens. To this end, ENISA is currently working on a European cybersecurity certification framework as part of which cybersecurity certification schemes will be established.

ENISA has designed this survey to capture the plans of your organisation to use the cybersecurity certification framework and the level of preparedness of your organisation in the uptake of the cybersecurity certification schemes. The survey also gives you the opportunity to indicate areas in which ENISA could provide (more) information and assistance to facilitate the use of the cybersecurity certification framework.

The completion of the survey takes approximately 10 minutes. They survey will be available from **15 December 2022** to **15 January 2023**.

Your answers to this survey are very much appreciated, and will allow ENISA to further improve its activities and to ensure the added value of its support to the European cybersecurity market, industry and stakeholders.

Should you have any questions on the survey, please do not hesitate to contact us via MCSsurveys@enisa.europa.eu .

Thank you very much for your time and valuable feedback!

Kind regards,

ENISA

Data privacy statement

Before you start: Privacy statement for this EU survey

Your personal data shall be processed in accordance with the Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.
The data controller of the processing activity is the Commission, DG CNECT.
The legal basis for the processing activity is Article 5(1) (a) of Regulation (EU) 2018/1725 which provides that "processing is necessary for performance of tasks carried out in the public interest", on the basis of Article 5 (5a) of Regulation (EU) 2019/881 (Cybersecurity Act), which tasks ENISA "to contribute to the development and implementation of Union policy in the field of electronic identity and trust services". In addition, the legal basis for the processing activity of acknowledging the survey participants in the report to be produced is Article 5(1) (d) of Regulation (EU) 2018/1725 which provides that "the data subject has given consent to the processing of his or her personal data".
The purpose of this processing activity is to gather feedback from the European Cybersecurity Certification Group on the Union Rolling Work Programme.
The data processor of this processing operation is the European Commission's EUSurvey (https://ec.europa.eu/eusurvey/), the platform used for the conduction of the survey. Sub-processor is the EU Agency for Cybersecurity (ENISA), the Market, Certification and Standardization Unit.
The following (personal) data related to participants are being processed by EUsurvey:

- ***Invitation number***
- ***Contribution ID***
- ***Username***
- ***Creation Date, Last update***
- ***The email address from which the survey was submitted***

Note: the content of the survey is strictly related to professional information and is not expected to include any further personal data of the survey participants.
Only designated ENISA staff involved in the data processing operation, will have access to the data, as well as designated staff of the data processor, which supports the data processing operation.
The data may also be made available to EU bodies charged with monitoring or inspection tasks in application of EU law (e.g. internal audits, European Anti-fraud Office – OLAF).
Personal data will be kept up to a maximum period of three months after the publication of the final ENISA's report on the topic.
You have the right of access to your personal data and to relevant information concerning how we use it. You have the right to rectify your personal data. Under certain conditions, you have the right to ask that we delete your personal data or restrict its use. You have the right to object to our processing of your personal data, on grounds relating to your particular situation, at any time. We will consider your request, take a decision and communicate it to you.
If you have any queries concerning the processing of your personal data, you can send an email to ENISA Data Protection Office: dataprotection@enisa.europa.eu.

☑ I confirm to have read the privacy statement and provide my consent to process the data in accordance with the privacy statement.

SECTION 1: Stakeholder' profile

Please select the category of stakeholder that you identify with:

- ○ Citizens
- ◉ Certificate consumers such as governments and businesses

SECTION 2: Level of knowledge/ awareness of the European cybersecurity certification framework

How familiar are you with the European cybersecurity certification policy framework?

- ○ Not familiar at all
- ◉ Have heard of it, but don't know the details
- ○ Familiar

Do you agree that the EU cybersecurity certification framework contributes to society in terms of improving cybersecurity, better cybersecurity awareness, and better cybersecurity resilience?

- ○ Strongly disagree
- ○ Mostly disagree
- ◉ Mostly agree
- ○ Strongly agree

SECTION 3: Trust in digital solutions

Does the notion of a **product** / **service certified** in the EU according to a cybersecurity certification scheme as compared to a **non-certified** one, have an **impact on your decision** to trust it?

- ◉ Yes
- ○ No
- ○ No difference

Does the notion of a **product** / **service labelled as certified** in the EU according to a cybersecurity certification scheme as compared to a **non-labelled** one have an impact on your decision to trust it?

- ◉ Yes
- ○ No
- ○ No difference

Is your decision to trust a **product or service that is certified** and possibly l**abelled** according to a cybersecurity certification scheme impacted if it is used by specific categories of users including minors ?

- ○ Yes
- ○ No
- ◉ No difference

Do you see a need for mandatory cybersecurity certification for specific categories of users including minors ?

- ◉ Yes
- ○ No
- ○ No difference

Does the provenance of certification impact your decision to trust a certified/labelled product or service e.g. whether certification originates from the EU or not?

- (●) Yes
- ( ) No
- ( ) No difference

Would you expect mandatory information disclosures in relation to a cybersecurity scheme for specific categories of users including minors ?

- (●) Yes
- ( ) No
- ( ) No difference

SECTION 4: Assistance for the use of guidance and recommendations

Manufacturers or providers will provide necessary documentation on guidance and recommendations to assist end users with secure configuration, installation, deployment, operation and maintenance.
Do you intend to use such information?

- (●) Yes
- ( ) No
- ( ) I do not know

How could ENISA improve the information/awareness of citizens on their cybersecurity choices?

- [x] By defining a label to help identify certified products
- [ ] By defining specific criteria for consumers (such as quality and accessibility of documentation, ease of use, …)
- [x] By working with consumer organizations on the interpretations of certification results to make them more accessible
- [ ] Other

In the TG VHCS we want to promote the use of a Common Security Advisory Framework (CSAF) widely used by the industry and Member States.

Do you use the Common Security Advisory Framework (CSAF) in your organization for your internal or external security advisories?.

- ( ) Yes
- (●) No

Do you use other advisory framework?

- ( ) Yes
- (●) No

Please provide any other information / comments in the box below

250 character(s) maximum

Contact

Contact Form