

Privacy Statement - EU CyberSecurity Index Platform

Your personal data shall be processed in accordance with 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.¹

The data controller of the processing operation is ENISA Knowledge and Information Team. In certain Index, co-organised with other entities, such as other EU bodies or EU Member State Authorities, ENISA Core Operations Department and the co-organising authority(ies) are joint controllers. In such cases, further specific information will be provided by the co-organising entities, setting out the roles and responsibilities of each entity.

The legal basis for the processing operation is Article 5(1)(a) of Regulation 2018/1725 (necessary for performance of tasks in the public interest attributed by EU legislation) based on the *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, and *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) (NIS 2 Directive)* in particular, Article 18:

1. *ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following:*
 - (a) *a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape;*
 - (b) *an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union;*
 - (c) *an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises;*
 - (d) *an aggregated assessment of the outcome of the peer reviews referred to in Article 19;*
 - (e) *an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.*
2. *The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.*
3. *ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e)*

¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002.

In order to facilitate and manage such EU Index ENISA has developed an online platform called the Cybersecurity Index (EU-CSI) Platform.

The purpose of this processing operation is to manage and operate all projects relevant to the ENISA's cyber Index, e.g. organising planning events, sending survey, evaluating an Index, etc.

The following personal data are collected for all users of the platform:

- a) *Contact data*: name, surname, professional e-mail address, country, and telephone number*. (* denotes optional data). These data are necessary for establishing a user's account in the INDEX platform and/or organising Index-related events, such as planning workshops.
- b) *Index-related data*: while participating in different Index projects a user may produce data in the platform related to these projects, for example data related to his or her knowledge, opinion or analysis in the field of information security or data related to the evaluation of a specific Index project, e.g. by filling in relevant evaluation surveys, quizzes, reports etc. These data are optional and subject to the participation of the user in a specific Index-related project.
- c) *Platform logging and monitoring data*: events and actions in the INDEX are logged and monitored for performance and security reasons, such events may include participants' successful log-in/log-out, failed log-in attempts, etc.

The recipients of the data are designated ENISA staff and contractors involved in the overall management and operation of INDEX, as well as designated INDEX users that are involved in the management of specific Index projects. The data may also be available to EU bodies charged with monitoring or inspection tasks in application of EU law (e.g., internal audits, European Anti-fraud Office – OLAF). **The name, surname, email, and country are readable by all platform users.** During the execution of an Index, the contact data of the users who are players are shared with the other users who are participants in the same Index, in order to contain communication within the Index only.

All personal data will be kept up to **six months** after the finalisation of the evaluation report of the last Index project that a user participates in. Backup data may be kept for a maximum of **two years after** the planned execution of the Index for security reasons. After this period, all contact data are automatically deleted, while Index-related and logging/monitoring data are kept in anonymised form.

You have the right to access your personal data, the right to correct any inaccurate or incomplete personal data and the right to delete your data. If you decide to have your account deleted, contact data will be deleted from the INDEX platform within at most one week. Index-related data will be kept in anonymised form (without linking to contact data). If you have any queries concerning the processing of your personal data, you may address them to ENISA's EU-CSI team e-mail address: security-index@enisa.europa.eu.

You shall have right of recourse at any time to the ENISA Data Protection Officer (DPO) at dataprotection@enisa.europa.eu and to the European Data Protection Supervisor at <https://edps.europa.eu>.