European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

ENISA CYBER EXERCISES PLATFORM

Record of processing activity

Title	ENISA Cyber Exercises Platform
Name and contact details of controller	ENISA, Core Operations Department, exercises@enisa.europa.eu
Name and contact details of DPO	dataprotection@enisa.europa.eu
Name and contact details of Joint Controller	For exercises co-organised with other entities, such as other EU bodies or EU Member State (MS) authorities, the co-organising authority(ies) are joint controllers. For example: eu-LISA (security-exercises@eulisa.europa.eu). For certain exercises jointly planned with EU MS authorities, such as the Cyber Europe series of exercises, the designated entities, such as EU MS authorities, who have been delegated the responsibility to manage the participation of other entities in projects hosted in CEP – for example exercise planning authority – are joint controllers sharing responsibility for the protection of personal data. Their access is limited to the data of the exercise(s), which they manage or plan.
Name and contact details of processor	Outsourced contractors involved in the overall management and operation of CEP. Provider of Cloud infrastructure supporting CEP:Microsoft Azure, used under SLA between ENISA and European Commission DG DIGIT for the Cloud II Framework Contract (DIGIT-00786-00).
Purpose of the processing	According to Article 6 of ENISA's Regulation (EU) 2019/881, one of ENISA's task is to support capability building by supporting the organisation and running of Union network and information security exercises and, at their request, advising Member States on national exercises. In order to facilitate and manage such exercises ENISA has developed the cloud-based online Cyber Exercise Platform (CEP).
Description of data subjects	Organisers, participants, observers, contributors of any project hosted on CEP (users of CEP).
Description of data categories	The following personal data are collected for all users of the platform: a) Contact data: name, surname, business function*, affiliation*, sector, business address*, country, phone number(s), fax number*, e-mail information, photo* and business website*. (* denotes optional data). These data are necessary for establishing a user's account in the CEP platform and/or organising exercise-related events. b) Exercise-related data: while participating in different exercise 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 exercise 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 exercise-related project. c) Platform logging and monitoring data: Events and actions in the CEP are logged and monitored for performance and security reasons, such events may include participants successful log-in/log-out, failed log-in attempts etc.

Time limits (for the erasure of data)	Personal data can be removed from CEP either by controllers or by the data owner directly using the "forget-me" functionality. All personal data will be kept up to six months after the finalisation of the evaluation report of the last exercise project that a user participates in. Backup data maybe kept for a maximum of two years after the planned execution of the exercise. After this period, contact data are automatically deleted while exercise-related and logging/monitoring data, are kept anonymised.
Data recipients	Designated ENISA staff involved in exercise activities; designated staff of ENISA contractors (data processors).
Transfers to third countries	Personal data are located in Microsoft Azure datacentres within EU. ENISA only uses the processor for infrastructure - IaaS (Microsoft Azure) for the CEP platform. Limited necessary transfers of personal data may take place to Microsoft datacentres in the US or elsewhere in the context of the service provision, e.g. for technical support. Transfers are performed on the basis of safeguards put in place by the EC DG DIGIT with Microsoft - under relevant Cloud II DG DIGIT Framework Contract.
Security measures - General description	There is a security policy, which documents in detail: the security system specification of CEP; viz. security architecture, webserver/database servers security, patch and update policy, password policy, backup policy, authentication, access control, user management policy, physical security and disaster recovery system monitoring and incident handling, roles, responsibilities, log monitoring, auditing, incident handling. For the IaaS provision (Micrsoft Azure), relevant security policies of the processor are in place (under DG DIGIT Cloud II FWC).
Privacy statement	General CEP privacy statement: https://www.cyberskills.eu/Resources/DataPrivacyStatement.pdf; Spefic privacy statements are provided per exercise by joint controllers.