European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

RECORD NO: 27

ENISA CYBER SECURITY TRAINING

Record 27 of processing operation "ENISA Cyber Security Trainings"	
Date of last update	25/07/2024
Name and contact details of controller	ENISA, Capacity Building Unit (CBU), Trainings and Exercises Sector, trex [at] enisa.europa .eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	Provider of Cloud infrastructure supporting the trainings (for some trainings only): Microsoft Azure and Amazon Web Services (IaaS), used under SLA between ENISA and European Commission DG DIGIT for the Cloud II Framework Contract (DIGIT-00786-00). Third party trainings are provided as a service by Rangeforce or through the specific contract S-COD-20-C33 (External Cloud based Technical Training Services).
Purpose of the processing	ENISA collects and processes personal data of training participants to deliver and manage cybersecurity training programs. This information is essential for participant registration, training material distribution, certificate issuance, and quality assessment. When participants utilize our cloud-based training platform, account creation is necessary for platform access and interaction. For training provided by third-party service providers like Rangeforce, depending on the date of electronic registration • Prior to July 25, 2024, participants had two registration options: Alias account: participants could reuest a unique "training" account (alias UID) to interact with the platform without revealing their real email addresses to the service provider. ENISA maintains a secure record linking these training accounts to corresponding real email addresses for administrative purposes. Certificate issuance by the provider was not supported for alias accounts. Email account: participants could opt to provide their real email addresses for direct platform access. In this case, the service provider collected their name and email address to facilitate certificate issuance and potentially expedite support interactions. • Effective July 26, 2024, only the email account option is available. As intermediate administrators in the third-party platform, ENISA has access to participants' training record (viz. module completion and attempts), which is used for aggregated analysis and not for individual tracking. Coaches designated by Member State authorities or stakeholder organisations for their trainees can also view this information and assign training objectives; limited to the groups or individuals they have been assigned to. By default, only training accounts are visible to ENISA administrators through the platform. However, if participants use their real email

	addresses, their associated data (at a minimum, email address) will be visible within the platform's administrative overview. ENISA's primary focus, for the collection collect and processing personal data, is on delivering effective training and assessing program quality. Data handling is limited to the purposes outlined above.
Description of data subjects	ENISA stakeholders from EU Member States (public and private organisations) and other EU Institutions who attend the training courses.
Description of data categories	Personal data which is required for the management of training events. Such data includes name, surname, business function, affiliation, sector, country, phone number, mobile number and e-mail address. In addition, basic information for user account creation and management is required to provide access and use (of training participants) to cloud-based training platform. All of the above data will be kept by ENISA only. Third party trainings (Rangeforce) will require the end-user's name and email address, only with the user's consent (opt-in). Otherwise, a pseudonym will be provided to Rangeforce, produced by ENISA. ENISA will host the data collating the pseudonym to the user's email address.
Time limits (for the erasure of data)	Five years after the end of the training course, in order to provide an overview of the trainees for auditing purposes.
Data recipients	ENISA desiganted staff only and designated staff of data processors. Data cannot be disclosed to any third party for any reason without the prior consent of a user.
Transfers to third countries	Regarding the cloud-based training platform: personal data of training participants (user accounts) are located in Microsoft Azure datacentres within EU. Personal data of ENISA staff (admins) are located in Microsoft Azure and AWS datacenters within EU. Limited necessary transfers of personal data may take place to Microsoft or AWS in US or other third countries, as required for the service provision, e.g. technical support. Transfers are performed based on safeguards put in place by EC DG DIGIT with the service providers- under relevant Cloud II DG DIGIT Framework Contract. The Rangeforce trainings platform do not involve personal data transfers outside EU. The support mechanism also provides assurances that only staff located in EU will access the User information (support related emails).
Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's internal IT systems and ENISA's website. Security measures of AWS and Microsoft Azure platforms (IaaS services), as covered under the Cloud II DG DIGIT Framework Contract. Security measures of the service provider (Rangeforce OÜ) for the third-party training platform.
Privacy statement	Provided to data subjects as part of registration to the trainings.