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

ENISA CYBER SECURITY TRAINING

Record of processing activity

Title	ENISA Cyber Security Training
Name and contact details of controller	ENISA, Capacity Building Unit (CBU), Trainings and Exercises Sector, trex@enisa.europa .eu
Name and contact details of DPO	dataprotection@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 provides cybersecurity training to interested parties. Personal data of the participants to the training are collected upon registration in order to provide good quality trainings and to prepare the required documentations (certificates of attendance, registration sheets, etc.). When using the cloud-based training platform, the training participants also need to create a user account, so as to be able to access and further use the platform. When using third-party trainings, the trainings are provided by the service provider (Rangeforce) for registered users (training participants). In the default configuration, the real email address of the participants will not be used by the service provider, instead ENISA will provide a special so called “training” account that provides participants access to the third-party training platform without further identification (by the service provider). ENISA will maintain a table that links the real email addresses of participants to their respective training account but only for the above-mentioned reasons. Alternatively, the participants can choose to use their real email addresses on a voluntary basis to access the third-party training platform and their name will be collected by the service provider. In such cases, in addition to the above-mentioned reasons for collecting (and processing) personal data in the context of the training, the email address and name will be used by the service provider to send participants that successfully concluded training modules a certificate (created by the service provider). Support requests that are triggered from within the platform can potentially be solved faster in such case, since a 1-1 communication between the participant and the support staff of the third-party provider can be initiated (whilst in the default configuration, all support related communication would have to be handled via ENISA as an intermediate proxy). As intermediate administrators in the third-party platform, ENISA has access to an overview of what modules any given participant has engaged and successfully concluded, a functionality ENISA is not actively using since only aggregated data is of relevance for ENISA. In the default configuration, only the training account would be displayed to the ENISA’s administrators. In case that participants choose to use their own email address, participants will be present in this overview with the data they chose to provide to the third-party provider (at least their email address) and ENISA.

Description of data subjects	ENISA stakeholders from EU Member States (public and private organisations) 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 upon registration to trainings.